PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/00 — A2

(11) International Publication Number: **WO 98/41044**

(43) International Publication Date: 17 September 1998 (17.09.98)

(21) International Application Number: PCT/US98/05096

(22) International Filing Date: 13 March 1998 (13.03.98)

(30) Priority Data:
60/041,093 14 March 1997 (14.03.97) US

(71) Applicant: NORTHERN TELECOM INC. [US/US]; 2221 Lakeside Boulevard, Richardson, TX 75082-4399 (US).

(72) Inventors: YAU-FAN, Leung; 1604 Belgrade Drive, Plano, TX 75023 (US). DENMAN, Robert, E.; 2420 San Gabriel Drive, Plano, TX 75074 (US). WAMBSGANZ, Kevin; 1809 Papeete Drive, Plano, TX 75075 (US). CHANG, Kim; 3114 Park Gark Place, Richardson, TX 75082 (US).

(74) Agent: CARR, Gregory, W.; Winstead Sechrest & Minick P.C., 5400 Renaissance Tower, 1201 Elm Street, Dallas, TX 75270-2199 (US).

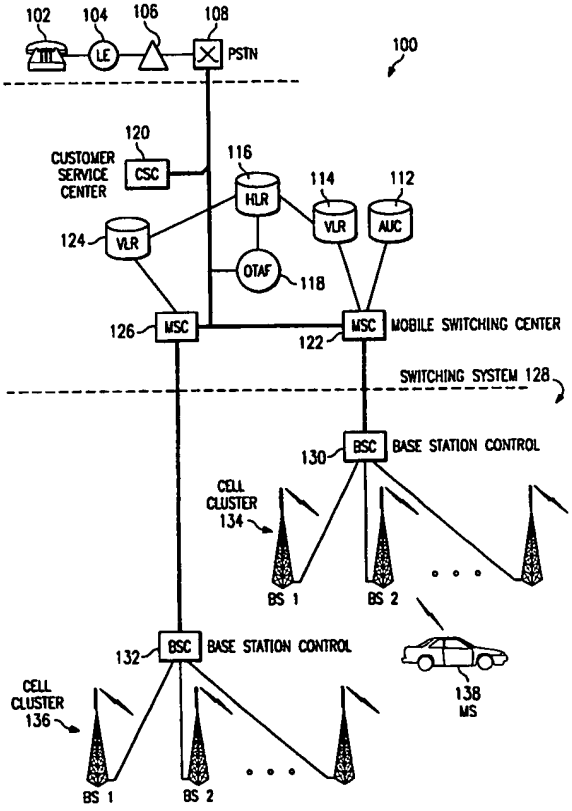
(81) Designated States: JP, KR.

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR NETWORK INITIATED PARAMETER UPDATING

(57) Abstract

Disclosed is an apparatus for initiating an over the air parameter administration (OTAPA) of a mobile station without the need for interacting with a mobile station user. A unique service option number included with the initial page indicates to the mobile station that an update is being requested. The mobile station performs a network validation check (SPASM) before permitting the update to take place. Flags are used in the network to alert the system that an attempted update was not completed because a mobile station was not update accessible for any of several reasons. The flags cause the system to update when the mobile station next becomes update accessible.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR NETWORK INITIATED PARAMETER UPDATING

TECHNICAL FIELD

The present invention relates in general to over-the-air parameter administration in a wireless communications network and, in particular, to network initiated communication of data using over-the-air parameter administration, whereby mobile stations may be provisioned and configured for service on a particular operator network.

BACKGROUND

With the advent of widespread use of cellular telephones and the corresponding growth of wireless subscribers for using such telephones, a need has arisen for providing services and modifying programmed information within each of the devices used by wireless subscribers. Before describing how this need has been addressed, however, a general structure of a wireless communications systems will be described. The infrastructure of a wireless communications network generally includes multiple mobile switching centers (MSCs) which provide wireless services, control, and tracking of mobile stations within a predetermined area.

The term "mobile station" (MS) as used in the remainder of this specification and the claims is intended to refer to any wireless communication device whether the device is mobile or fixed and whether used for the transmission of voice, data or facsimiles. Subscriber Unit is another term that is used in the art to describe such a device.

A home location register (HLR) is typically utilized in the infrastructure for a wireless communications network. For each MS it serves, the HLR retains a profile of information about the mobile station, including special features for which the mobile station is authorized and where the MS is currently located. A mobile station registers its location, in terms of a currently serving MSC, on its home HLR. An MSC that is currently serving a mobile station will retrieve the MS's profile from the HLR, and store the profile in a visiting location register (VLR) that is often co-located with the serving MSC.

Subsequently, when a call for a mobile station is received by a home network, the home HLR determines where to route the call. Through this method, the home network is able to transfer the call to the current visited MSC so that the mobile station receives the call even when it is not within its own home network.

In some wireless communication networks, a number assignment module (NAM) is implemented in each of the mobile stations. The NAM provides a memory for the mobile station to hold certain relevant information. That information may include a roaming list of available roaming systems, as well as certain operational parameters such as the mobile station's directory number. It should be noted that the parameters maintained in a mobile station's NAM are assigned by a service provider to control wireless network usage. Equivalent parameters in a wireline telephone network are completely under the control of the service provider and are not stored in equipment belonging to the subscriber. However, because wireless technology breaks the direct link between a mobile station and the communication network, some operational parameters must be stored in the mobile station. As a result, wireless service providers have historically accepted a loss of control over NAM parameters once initial programming is complete.

Typically, the NAM is programmed when a mobile station is first activated. For example, before a mobile station is first utilized, the NAM is programmed by the service provider to have a preselected roaming list, services, and a directory number to be associated with the mobile station itself.

When any of the network-stored parameters that were used to supply data originally programmed into the NAM are modified, those modifications must be reflected by modifying the NAM so that the mobile station may operate correctly. In such a situation, the subscribers are typically required to physically take the mobile station to a location specified by the service provider for NAM reprogramming. Alternatively, an Over-The-Air Service Provisioning (OTASP) mechanism may be used to either activate a new mobile station, modify the existing services provided to a subscriber, or update the existing operation parameters without the intervention of a third party. OTASP is defined in a telecommunication industry association (TIA) standards having designations of IS-683 and IS-725. However, the OTASP mechanism, as specified in IS-683 and IS-725, is initiated only by the subscriber. Furthermore, the OTASP mechanism may require connection to a customer service center of a service provider for interaction with a customer service representative. Thus, while OTASP sessions do not require the mobile subscriber to physically take their mobile stations to a location specified by the service provider, subscriber effort is still required to accomplish the updating process.

Additionally, with the use of the OTASP mechanism, security may become an issue. Specifically, a wireless service provider should be able to insure that the NAM is not programmed from a renegade source. In the OTASP mechanism, a service program lock (SPL) procedure is utilized. In the SPL procedure, a password is sent to the mobile station and then used to "unlock" the mobile station if the password corresponds to that stored in the mobile station. If the password does not correspond to that stored in the mobile station, the message and programming effort is rejected. However, a lock procedure, such as SPL, where a given password is transmitted over the air, is subject to unauthorized interception. Thus any over-the-air transmitted passwords or unlocking signatures may need to be altered with each transmission to lower the risk of improper usage of such passwords by unauthorized entities.

Therefore, in addition to the need to easily program a mobile station within a wireless communication network, there exists a need to insure that such programming is performed in a secure manner such that a subscriber's mobile station is not "hijacked" for unauthorized purposes. Furthermore, a need exists for a programming methodology that may be easily implemented with minimal interruption and inconvenience to the wireless subscriber.

SUMMARY OF THE INVENTION

The present invention provides a secure method and apparatus for updating operational parameters in a mobile station as initiated by the associated network.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates, in block diagram form, a wireless communication network in accordance with one embodiment to the present invention;

FIGURE 2 illustrates, in a time sequence diagram form, a methodology of a prior art process designated as OTASP;

FIGURE 3 illustrates, in a time sequence diagram form, a generalized methodology of the updating process implemented in accordance with one embodiment to the present invention;

FIGURE 4 illustrates, in a time sequence diagram form, a generalized methodology of the updating process implemented in accordance with one embodiment to the present invention as between the MS and a base station (BS);

FIGURE 5 illustrates, in a time sequence diagram form, a generalized methodology of the updating process implemented in accordance with one embodiment to the present invention where the MS may be visiting a foreign system;

FIGURE 6 illustrates, in a time sequence diagram form, a more specific methodology implemented in accordance with one embodiment to the present invention where the paging channel and the access channel are used to perform the update;

FIGURE 7 illustrates, in a time sequence diagram form, a more specific methodology implemented in accordance with a further embodiment to the present invention where the paging channel and the access channel are used to perform the update;

FIGURE 8 illustrates, in a time sequence diagram form, a more specific methodology implemented in accordance with one embodiment to the present invention where traffic channels are used to perform the update;

FIGURE 9 illustrates, in a time sequence diagram form, a more specific methodology implemented in accordance with a further embodiment to the present invention where traffic channels are used to perform the update;

FIGURE 10 illustrates, in a time sequence diagram form, a more specific methodology implemented in accordance with one embodiment to the present invention where a traffic channel is used to perform the update while the MS is on call;

FIGURE 11 illustrates, in a time sequence diagram form, a more specific methodology implemented in accordance with a further embodiment to the present invention where a traffic channel is used to perform the update while the MS is on call;

FIGURE 12 illustrates, in a time sequence diagram form, a methodology of validating the network attempting to perform an update;

FIGURE 13 illustrates, in flow chart form, one embodiment of a network validation process used in the present invention;

FIGURE 14 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention when a mobile station cannot be located;

FIGURE 15 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention when a mobile station is unavailable;

FIGURE 16 illustrates, in a time sequence diagram form, a methodology implemented in accordance with a further embodiment of the present invention when a mobile station is unavailable;

FIGURE 17 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention when a mobile station accesses the system after an OTAPA flag has been set;

FIGURE 18 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention where a mobile station roams between OTAPA capable systems after an OTAPA flag has been set;

FIGURE 19 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention where a mobile station roams into an OTAPA incapable systems after an OTAPA flag has been set;

FIGURE 20 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention where an MSC transfers an OTAPA pending flag to the HLR when a mobile station becomes inactive;

FIGURE 21 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention where an HLR does not have the location information of a mobile station;

FIGURE 22 illustrates, in a time sequence diagram form, a methodology implemented in accordance with a second embodiment of the present invention where an HLR does not have the location information of a mobile station;

FIGURE 23 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention where a mobile station registers after an OTAPA pending flag has been set at an HLR;

FIGURE 24 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention where a OTASP call is initiated after an OTAPA pending flag has been set at an MSC;

FIGURE 25 illustrates, in a time sequence diagram form, a methodology implemented in accordance with a further embodiment of the present invention where an OTASP call is initiated after an OTAPA pending flag has been set at an MSC;

FIGURE 26 illustrates, in a time sequence diagram form, a methodology implemented in accordance with one embodiment of the present invention where an OTAPA process is enabled while the mobile station is in a system where it is inappropriate to perform OTAPA;

FIGURE 27 illustrates, in a time sequence diagram form, a methodology implemented in accordance with a second embodiment of the present invention where an OTAPA process is enabled while the mobile station is in a system where it is inappropriate to perform OTAPA; and

FIGURE 28 illustrates, in a time sequence diagram form, a generalized methodology applied to the situation where an OTAPA process is enabled when the mobile station is in a situation where OTAPA cannot be performed at that time.

DETAILED DESCRIPTION

The present invention sets forth a communication network and methodology for implementing an over-the-air parameter administration (OTAPA) methodology wherein a wireless communication service provider may modify service information stored within a wireless subscriber's mobile station without requiring that the subscriber be notified or take certain actions. Specifically, the OTAPA mechanism of the present invention simplifies administration of certain parameters, including values in a number assignment module (NAM), stored within a mobile station for both the service provider and the subscriber by allowing network-initiated over-the-air access to the parameters. Such access allows service providers to significantly improve customer care processes, while being totally unobtrusive to the subscriber. In addition, the present invention secures the mobile station's stored parameters from being modified by an unauthorized network.

Furthermore, the OTAPA mechanism implemented by the present invention does not require any interaction with the subscriber in order to be initiated or completed successfully. Additionally, the OTAPA mechanism of the present invention may be performed at any time the subscriber has an active mobile station, as long as the OTAPA process does not interfere with normal user operation of the device (e.g. placing or receiving telephone calls). The OTAPA mechanism of the present invention may be supported on digital channels and, optionally, on analog channels used within the communications network. Each of the functions implemented by the present invention will subsequently be described in greater detail. Prior to that description, however, a description of a typical wireless communications network in which the present invention may be implemented will be provided herein.

In the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be obvious to those skilled in the art that the present invention may be practiced without such specific details. In other instances, well-known circuits and devices have been shown in block diagram form in order not to obscure the present invention in unnecessary detail. For the most part, details concerning timing considerations and the like have been omitted inasmuch as such details are not necessary to obtain a complete understanding of the present invention and are within the skills of persons of ordinary skill in the relevant art.

As will be further realized, this invention applies to a plurality of wireless access technologies. While the invention is described using code division multiple access (CDMA) terminology, the comparable terms in the other wireless technologies will be obvious to one skilled in the art. As an example, paging and access channels in CDMA terminology are designated as control channels in Advanced Mobile Phone System (AMPS) terminology.

Refer now to the drawings wherein depicted elements are not necessarily shown to scale and wherein like or similar elements are designated by the same reference numeral through the several views.

FIGURE 1 illustrates a typical wireless communication system that may be used to implement the methodology of the present invention. In a communication network 100, a land line telephone 102 is coupled to a local exchange (LE) 104. The local exchange is then coupled to the public switched telephone network (PSTN) 108. The PSTN 108 is coupled to an operation center labeled customer service center (CSC) 120 and mobile switching centers (MSC) 122 and 126. The two MSC's 122 and 126 communicate with a home location register 116 through an over-the-air function (OTAF) block 118. The HLR is connected to communicate with an Authentication Center (AUC) 112 as well as with visitor location registers (VLR) 114 and 124. The VLR 114 is connected to and is used solely for visiting MSs under the purview of MSC 122 while VLR 124 is connected to MSC 126.

In the communication network of FIGURE 1, mobile switching centers (MSC) 122 and 126 communicate via HLR 116 with authentication center (AUC) 112 to insure that subscribers attempting to use communication network 100 are authorized to do so. It may be noted that an authentication center is also often referred to in the art and in an attached set of definitions by the acronym AC. It should be noted that all mobile station equipment used on communication network 100, whether a hand portable or vehicle-mounted phone or other

wireless communication device, stores an identification number referred to as a mobile station identification (MSID). An MSID may be MIN or IMSI as defined in the attached appendix. The MSID is typically programmed into the mobile station during the activation process performed by a service provider.

During operation of communication network 100, base stations (BS) communicate data to a mobile subscriber at mobile station (MS) 138. Such base stations are typically arranged in clusters (134, 136) that are controlled using a base station controller (BSC). For example, BSC 130 controls operation of cell cluster 134 and BSC 132 controls operation of cell cluster 136. Mobile switching centers 122 and 126 are implemented to direct traffic around the network. Each mobile switching center is associated with a home location register (HLR) 116 and a visiting location register (VLR). For instance, MSC 126 is associated with VLR 124 and MSC 122 is associated with VLR 114. It should be noted that each MSC is not necessarily physically associated with a corresponding VLR.

Another network entity that is typically connected to the HLR is the over-the-air function (OTAF). OTAF is the network entity that supervises the over-the-air service provisioning upon requested by the customer service center (CSC). The OTAF receives the mobile station's updated information from the CSC and then interacts with the serving MSC to download the information to the mobile station. Standard operation of each of the elements of communication network 100 is well-known to those with skill on the art and, therefore, will not be described in greater detail herein.

The present invention implements an over-the-air parameter administration (OTAPA) methodology that allows a service provider, such as that embodied in customer service center (CSC) 120 of FIGURE 1, to update certain parameters stored within a mobile subscriber such as mobile subscriber 138 of FIGURE 1. The parameters to be modified may be various NAM indicators, as well as roaming lists and other information typically stored within a memory of a mobile subscriber.

In contrast to previously implemented methodologies for modifying information stored within a mobile station, the OTAPA mechanism of the present invention is a network-initiated programming procedure. The OTAPA programming procedure of the present invention uses an existing over-the-air programming protocol that supports a previously implemented OTASP feature to provide a very different network-initiated programming procedure. Furthermore, the present invention implements a mobile station parameter administration security mechanism

(SPASM) that prevents an unauthorized network-initiated over-the-air programming from being performed. In the event that an MS has a plurality of NAMs, each NAM in that MS is secured separately using the SPASM protocol.

To contrast the functionality of the OTAPA methodology of the present invention, a prior art OTASP methodology will be generally described. FIGURE 2 illustrates a typical OTASP call flow that describes the communications made between a mobile station and a base station. In a typical prior art OTASP call flow, a mobile subscriber originates the OTASP mechanism by placing a call via a local base station to a specified service provider customer service center such as 120 in FIGURE 1. Subsequently, channel assignment and service negotiation functions occur between the mobile station and the base station to form a communications channel. Such channel assignment and service negotiation functions are well-known to those with skill in the relevant art.

Subsequently, the base station may access the capability of the mobile station by sending a protocol capability request message. The protocol capability request message basically ascertains the functionality supported by the mobile station. After the mobile station provides this functionality to the base station through a protocol capability response message, a service programming lock procedure is initiated in which the wireless communication device corresponding to the mobile subscriber is "unlocked" for programming. In the lock procedures implemented by typical OTASP communication systems, the base station will send a message having a password embedded therein to the mobile station. The mobile station compares the password to an internally stored password to determine whether external programming should be allowed. Should the password be correct and over-the-air (OTA) programming be allowed, the base station will proceed to program the mobile station with the appropriate information. After the base station has finished programming the mobile station, the base station generates a release order to release the traffic channel between the mobile station and itself. The release order completes the OTASP session. The foregoing OTASP call flow illustrates a traditional prior art method used to program the mobile station.

In contrast to above-described OTASP call flow that requires third party intervention by a service provider, the present invention implements an over-the-air parameter administration (OTAPA) methodology that allows a service provider to modify information stored within a wireless communication device of a mobile subscriber without requiring any action by the subscriber. Stated another way, the OTAPA methodology of the present

invention is initiated by the service provider and is virtually "transparent" to the subscriber. The methodology will subsequently be described in greater detail.

In FIGURE 3, an over the air function entity determines that an updating procedure is required. Typically the OTAF would be associated with the CSC of the home network of the MS such as CSC 120 and OTAF 118 of FIGURE 1. A message is sent, as shown, from the OTAF to the BS presently communicating with the MS that requires updating.

If the MS is idle, a general page message is sent to the MS with a service option (SO) indicator signifying that an OTAPA update is about to be performed. Upon receipt of the message, the MS sets a SO flag so that when a channel is assigned, the MS will not bother the user by supplying an audio "ring" indication. The MS then supplies a page response message and a channel assignment message is returned. The remaining actions illustrated in this figure are set forth in more detail in later figures.

If the MS already has a traffic channel assigned and is presently communicating with another entity on the traffic channel, there is no need to set up a traffic channel and signalling traffic will be used to commence the OTAPA function with an OTA Data Message. Most digital MSs in present use have the capability of multiplexing main and signalling communications with a BS. Many BSs can communicate over primary, secondary and signalling portions of a traffic channel simultaneously in a multiplexed manner.

In FIGURE 4, the OTAPA call flow is shown in more detail than in FIGURE 3 from the time when the base station pages the mobile station. The base station pages the mobile station to determine a location of the mobile station. The page response provides the base station with the mobile station's location.

Upon identifying the location of a given mobile station, the base station performs a channel assignment function in a manner similar to that used in the previously described OTASP call flow. While the channel assignment function may be similar to previously described channel assignment mechanisms, the service negotiation steps implemented by the present invention are significantly different than those previously implemented. Specifically, the present invention implements a unique service option number in the OTAPA communication protocol. Since the prior art updating with OTASP was user initiated, a regular voice service option number was used. The service option numbers and any accompanying data are communicated between the base station and the mobile station to provide detailed information about the data to be communicated. For example, the service

option numbers may indicate that the data being transferred between the base station and the mobile station is data associated with one of a voice call, a data call, or a fax/video call.

By implementing service option numbers that differentiate between an OTAPA call and a normal voice call, the present invention allows service providers to modify information stored internally within a mobile station without requiring the mobile subscriber to be aware of the modifications or to require the mobile subscriber to take certain actions. Stated another way, by implementing a unique service option number for an OTAPA call, a mobile device may be designed to recognize an OTAPA call and to perform preselected steps in response thereto, wherein one of the preselected steps may be to respond to the call without alerting the user of the mobile device. A more detailed description of service option number usage will subsequently be provided.

After the mobile station responds to the unique service option number in the OTAPA call and is assigned to a traffic channel (where the system design uses a traffic channel as opposed to the use of paging channels), a protocol capability communication may be transacted between the base station and the mobile station to determine the capabilities of the mobile station. It should be noted that the protocol capability message is not required and other OTA Data Messages may be used instead to initiate the OTAPA procedure in an alternate embodiment of the OTAPA methodology of the present invention.

At this point in the OTAPA methodology, a SPASM (Subscriber Parameter Administration Security Mechanism) may be implemented. SPASM is a security mechanism that protects parameters and indicators of active NAM within the mobile station from programming by an unauthorized network entity during the duration of the OTAPA function. As illustrated in FIGURE 4, the SPASM procedure may be executed either before, during or after the previously discussed capability request/response protocol is transacted. The SPASM procedure is, in a preferred embodiment, performed as part of the protocol capability communication and will subsequently be described in greater detail.

Referring again to FIGURE 4, the service programming lock procedure is performed after the SPASM procedure in one embodiment of the OTAPA mechanism of the present invention. As previously discussed, if a mobile device is locked by a service programming lock function, then the mobile station must be unlocked before its NAM may be programmed. In the OTAPA mechanism of the present invention, the OTA programming procedure is initiated to program the mobile station. After completion of the OTA programming procedure,

the base station communicates a release command to the mobile station and the OTAPA session is completed.

The network-initiated characteristics and the SPASM protocol of the OTAPA mechanism of the present invention were generally described above. A more detailed description of each of these facets of the present invention will subsequently be described. A general list of terms and definitions used in the following discussion has been excerpted from a draft version of the TIA/EIA/IS-683-A specification entitled "Over-the-air Service Provisioning of Mobile Stations in Spread Spectrum Systems," and is attached hereto in Appendix A.

In FIGURE 5, the initiation and completion steps of an OTAPA procedure are illustrated in general. The home CSC initiates the OTAPA process by informing the OTAF that a given MS needs an update. The OTAF queries the HLR for that MSs availability and the address of the MSC in which the MS is presently (or was last) operating. This information is returned to the OTAF. As will be apparent to those skilled in the art, this invention reuses existing intersystem messages that are being used today for Short Message Service (SMS). The OTAF then forwards a request to the indicated MSC. This request includes not only the OTAPA service indicator (SRVIND) but also the OTASP data message that would have been provided in the prior art user initiated OTA process. As indicated previously, OTAPA may be performed whether the MS is idle or is being used actively on a traffic channel. Preferably SPASM is performed to validate the network attempting the update and then the OTA programming is performed to complete the updating operation.

A release message is supplied from the OTAF to the MSC/BS. If the MS user is not presently involved in an active call, the traffic channel is released. Whether or not the traffic channel is released, the MSC/BS returns a response to the OTAF indicating receipt of the release message.

In FIGURE 6, a time sequence diagram presentation illustrates in detail the steps involved in completing the OTAPA process where the MS is idle and the paging channel is used to provide the update. As shown, the CSC enables the OTAF which transmits a request to the HLR as previously shown in FIGURE 5. (A superscript "1" was inserted in the figure to call attention that in various implementations this could be an OTASP notification or request as opposed to a SMS notification or request.) As will be detailed later, the HLR may set a flag indicating a pending OTAPA process and store the OTAF address in the event that

the OTAPA process is not successfully completed at this time. (The superscript "2" was inserted to indicate that alternatively, the MSC could set an OTAPA pending flag and store the OTAF address, so that if programming of the mobile is not successfully completed, provisioning may be continued at a later time when notified by the MSC.) The MSC/BS returns a message as shown providing various datum including the MSs mobile station identification (MSID). (The superscripts 3 and 4 have been included to indicate that although the some of the mnemonics in the messages appear to be the same, the min^3 is for the MS's identification and the min^4 is an activation MIN. However, as is known to those in the art, these two "min"s may be identical.) Thus the OTAF may be assured that the appropriate MS was contacted. The OTAF then returns an activation MSID along with other data such that the MSC/BS will page the MS with a SO indicator that signifies that an update or OTAPA process is to be performed. (The superscript 5 is used to indicate that alternatively the base station may choose to broadcast the data burst message which contains the protocol capability request message throughout the area where the mobile is last registered. However, paging the mobile has the advantage that the MS can be authenticated to verify its identity and paging is more efficient for messages sent to an MS operating in the slotted mode. The further superscript 6 indicates that while OTASP was previously performed, there was never a service option number assigned for that function.) After the page response, a protocol capability request message is transmitted between the MSC/BS and the MS. The protocol capability request message notifies the MS of the start of the OTASP session. A network validation on the order of the previously mentioned SPASM may be performed. SPASM is initiated with the base station challenge message. As shown in FIGURE 6, the Secret Shared Data (SSD) is available at the VLR. This reduces the time and cost required to complete the process. As noted in the box in this figure, if the shared secret data (SSD) is not shared, the VLR will forward the challenge via the mobile station's home HLR to the AC. SPASM will be described in more detail later.

If the MS obtains a satisfactory comparison of a returned authorization (AUTHBS) with its own internally generated AUTHBS, a satisfactory validation response message is transmitted to the OTAF as initiated by the protocol capability response message. The superscript 7 is used to indicate that a new field, result_code, should be introduced in the protocol capability response message from that previously used. If the AUTHBS received by the MS matches its own, the result_code is set to successful and the MS's protocol capability

is returned in the response message. The MS would then initiate the activation procedure since this means the OTAPA process is allowed. If , on the other hand, a mismatch occurs, the result_code is set to "rejected-AUTHBS mismatch (a new result code from that previously used) and thus the request to begin a OTAPA session is ignored.

An alternative way to handle the validation failure case is simply for the MS to not return the protocol capability response message and let the OTAF time-out on the smdpp message. However, OTAF can also time-out on smdpp messages due to various IS-41 network failures. Since the action taken by OTAF may be different for these failures, it is believed more appropriate to include the result-code in the protocol capability response message as indicated in the above paragraph.

Subsequently the update programming in completed. It may be noted however that the SPL may need to be unlocked per IS-683-A specifications in order to complete the programming process.

The superscript 8 is used to indicate that since the MSC has no "knowledge" of whether programming of the MS is completed or not, OTAF must inform the MSC of the completion of the OTAPA session. The MSC can then release the OTAPA session via the release order message. If the OTAPA pending flag is set as indicated previously in this figure in conjunction with superscript 2, the MSC clears the pending flag. Alternatively, this message can be sent directly to the MSC.

The MS may now be released. It may be noted that the release order is not required if the page message mentioned in conjunction with superscript 5 is not sent.

In FIGURE 7, a time sequence diagram presentation illustrates the steps involved in completing a preferred OTAPA process, alternative to that shown in FIGURE 6, where the MS is idle and the paging channel is used to provide the update. The process commences as was shown in FIGURE 6 when the mobile station's location information is requested by the OTAF. However, in contrast to the procedure in FIGURE 6, the request is not forwarded to the serving MSC and the information is returned directly from the HLR to the OTAF. The OTAF then sends a message directly to the serving MSC whether it be a home MSC or a visited MSC. As was the case in FIGURE 6, the mobile is idle and the OTAPA is to be performed using the paging/access channels. Once the mobile station is satisfactorily located by the MSC via paging, an OTAPA request message is sent from the MSC to the mobile station to initiate the OTAPA session and the SPASM process is completed in the manner shown in prior

figures. If necessary, the service programming lock procedure is then completed. After the completion of these two procedures,the mobile station parameters are updated in accordance with the essence of the OTASP process as illustrated in previous figures. OTAF finalizes the OTAPA process commencing with the request message on the line having the letter designation "r". The process in completed with the response message shown on the line designated as "u".

In FIGURE 8, the time sequence diagram shown again addresses the situation where the mobile station is idle when OTAPA is initiated. Thus a block shows that the process is the same as again FIGURE 6. After the visited MSC has been contacted and a reply returned to OTAF, a page is supplied to the mobile station in a manner similar to that of FIGURE 6. However, in this scenario, a traffic channel is assigned so that the OTAPA process is completed using a traffic channel rather than the paging/access process of FIGURE 6. The remainder of figure 8 operates in substantially the identical manner as that presented in FIGURE 6.

In FIGURE 9, the time sequence diagram uses the traffic channel in a preferred manner alternative to that of FIGURE 8 in the situation where the mobile station is idle. Thus the beginning of the process of FIGURE 9 is similar to the approach used in FIGURE 7. Once the OTAPA message is transmitted from the OTAF to the MSC, the mobile station is paged and moved to a traffic channel. The remainder of the procedure shown in FIGURE 9 is substantially identical to the remainder of FIGURE 7 in that the SPASM process, the service programming lock process and the OTASP process are all completed and the call is released.

It may be noted that one alternative way to handle the situation of a failure of the network validation process is that the mobile station simply not return the protocol capability response message. In such a situation the OTAF would timeout and know that the update had not been successfully initiated. However since the OTAF can timeout for other network failures it is believed more appropriate to provide the response message to the OTAF that the validation process has been completed in each of the FIGURES 6 through 9. It may be further noted that since the MSC does not receive data as to whether programming of the mobile station is completed or not, OTAF must inform the MSC of the completion of the OTAPA session. If an OTAPA pending flag is set in the MSC as shown at block 2 of FIGURE 6, the MSC simply clears the pending flag. Otherwise, the OTAF must send a message to release as specifically shown in FIGURE 6 and as implied in FIGURES 7.

In FIGURE 10, a time sequence diagram is presented for use in a situation where a mobile station is processing a call on the traffic channel. The process of FIGURE 10 is presented along the lines of FIGURES 6 and 8. As set forth before, the CSC enables the OTAPA process in a message to the OTAF. Messages are passed from the OTAF to the visited MSC and a reply is returned to the OTAF that the MSC has received the request. The MSC has knowledge that the mobile station is operating in a call mode and thus the MSC does not attempt to page the mobile station as set forth in FIGURE 8. When the MSC receives the return message from the OTAF, it does not supply a service option indicator to the mobile station. Rather the MSC merely requests the commencement of the protocol capability process. The mobile station performs a network validation as set forth previously. If the validation process is satisfactorily completed, the mobile station is updated in the manner previously set forth in FIGURE 8.

In FIGURE 11, the diagram is again presented for the situation where the mobile station to be updated is already using an assigned traffic channel as was assumed in connection with FIGURE 10. The OTAF, after being enabled by the CSC and after requesting data from the HLR, sends it and OTAPA request message to the visited MSC. An appropriate OTAPA request message is then transmitted from the MSC to the mobile station to commence the SPASM process. As set forth in FIGURE 10, there is no need for paging the mobile with a service option indicator. The remainder of the process of FIGURE 11 is substantially identical to that presented in FIGURE 9 except there is no need to release the call until the call presently in progress by the mobile station user has been completed.

As will be apparent to those skilled in the art, in the situations of either of the processes shown in FIGURES 10 and 11, when a call is completes, the update will not be completed if the downloaded data is never committed between the mobile station and the system. In the event such a failure does occur, the lack of an OTAPA response message from the mobile station as shown near the end of FIGURE 11 will cause the OTAF to timeout. The timeout of OTAF will cause it to set a flag as will be discussed later so that the OTAPA process is attempted again whereby the update process can be completed.

In a FIGURE 12, a time sequence diagram presentation is provided of the network validation scheme previously labeled as SPASM. This process is referenced in at least previous FIGURES 4, 5, 9 and 11. When the mobile station determines that an OTAPA session is being initiated, the mobile station challenges the system via base station challenge.

This base station challenge is forwarded to another entity to compute the authorization signature (AUTHBS) based on a secret word, preferably the secret shared data (SSD), appropriate to that mobile station which is normally stored in the home AC. The base station challenge, BSCHALL, in various embodiments, may be processed at the visiting location register, an OTAF or an AC depending on how the system is implemented, whether or not the visited network can be trusted by the home network, and where the secret word is available. Thus this figure shows HLR/AC in a solid box and a VLR in a dash line box to illustrate some variations of the concept. Once the validate signature is computed based on the secret word, it is returned to the base station which issues a response to the mobile station. Once the mobile station compares an internally generated signature with the received signature it provides an appropriate response to the base station.

Although the SPASM process can be performed in various degrees of complexity, the flow diagram of FIGURE 13, presents the concept in simplified terms. A signature is computed based on a secret word stored within the mobile station, preferably the SSD, and a randomly generated number, using a previously known CAVE algorithm. This random number is supplied to a network entity, preferably the home AC, for processing. As illustrated in FIGURE 13, since the secret word (SSD) is also available at the AC, a signature can be generated with the received random number in an identical algorithm. The generated signature may then be returned as part of the base station challenge confirmation order. If the signature generated within the mobile station is identical with the generated signature returned by the AC, the mobile station can assume that this is a valid network request. Subsequently, a trigger causes the initiation of the OTAPA process such as a protocol capability response (not shown) or the appropriate OTAPA response message is supplied to the entity requesting the OTAPA process. The simple validation process shown in FIGURE 13 may be made even more secure by first combining the secret word with further data known only to the AC before performing the CAVE process. It should be noted that the SSD used in FIGURE 13 can be substituted, in other embodiments, with another secret word that is only known to the mobile station and the AC.

As will be apparent to those skilled in the art, occasions will rise when the OTAPA process is initiated and the mobile station cannot be contacted for some reason or another. In FIGURE 14, the time sequence diagram is presented setting forth the actions taken by the various entities involved. After the OTAF has completed the OTAPA request to the MSC,

received a reply and then has returned a response to the MSC as set forth in either FIGURE 6 or FIGURE 7, the MSC will ascertain it has waited too long. In the words of art, it will "timeout". As illustrated in this FIGURE 14, the MSC stores the address of the OTAF and sets an OTAPA pending flag. The MSC then sends (returns) a "postponed" message to the OTAF. As it will be ascertained from figures to be yet discussed, if the MSC does not contact the mobile station within a predetermined time, the OTAF will be modified to store the OTAPA pending flag and the stored information will be cleared from the MSC register.

In a FIGURE 15, a slightly different scenario is addressed. In this figure the situation occurring that needs to be addressed is that the mobile station is unavailable for some reason such as it has not recently been in contact with the MSC. Typically the MSC will have attempted a page in the recent past and has been unsuccessful. As shown, the pending flag is set and the OTAF address is stored as occurred in FIGURE 14.

The time sequence diagram of FIGURE 16 presents a different approach to setting up an OTAPA pending flag in the MSC. As may be ascertained, in the approach used in this figure, the OTAF, after receiving the enablement message from the CSC, sends a request to the HLR. The HLR returns the appropriate information as to the address of the mobile station as most recently stored in the HLR. OTAF then sends a message to the MSC. Rather than responding with an answer message as shown in previous FIGURE 14, the MSC, in this embodiment, stores to the OTAF address sets the OTAPA pending flag and then sends a message back to the OTAF indicating that the OTAPA process has been postponed. In previous FIGURE 14 the postponement message was not returned until after a timeout occurred. As indicated on line f of FIGURE 16, system access is later attempted by the mobile station. At this time a notification message is returned to the OTAF entity from the MSC and OTAF completes the update process as illustrated in previous figures.

In FIGURE 17, the time sequence diagram presentation illustrates the message passing solution to a situation where a flag has been set such as illustrated in the previous FIGURES 14-16. When a mobile station subsequently accesses the system as shown by the system access message from the mobile station to the MSC near the top of this figure, the MSC notes the flag and sends a notification to the OTAF that the mobile station is now available. The situation presented here may cause this process to be followed whether the mobile station access is for origination, termination or registration. Once the OTAF has replied to the MSC, the OTAPA process can proceed in the manner previously discussed in accordance with

system parameters. In other words the system may do the updating with paging messages or with traffic messages and the entity completing the network validation process may be the visited network's VLR or the home AC. In any event the OTAPA pending flag is cleared from the MSC once the updating is completed.

In FIGURE 18, the time sequence diagram presentation illustrates the messages involved where the mobile station has roamed between OTAPA capable systems and the OTAPA pending flag has been set in the MSC of a previously visited system. The initial contact of a mobile station with an MSC in a visited system causes a known process designated as registration. The MSC in the newly visited system sends a registration notification message to the VLR. Since the system is new to the MS, the VLR forwards the notification request to the home system and the message eventually gets to the HLR. When the HLR sends a registration cancellation message to the previously visited MSC, the reply to the HLR includes the information that the OTAPA process is pending. The old MSC clears the pending flag and the HLR notifies the new MSC that as part of the registration process it should set a OTAPA pending flag and store the OTAF address. Once it registration is completed, the new MSC notifies OTAF that the mobile station is available and at the appropriate time the OTAF sends a protocol capability request and the process continues as previously set forth in FIGURES 15 or 16.

Alternatively, the HLR may notify the OTAF with a SMS notification message when it receives the registration cancellation message from the previously visited MSC containing the OTAPA pending information. It is believed obvious to one skilled in the art that this variation could be practiced without providing a separate figure setting this sequence forth explicitly.

The time sequence diagram of FIGURE 19 addresses the situation where a mobile station roams into an OTAPA incapable system when the OTAPA pending flag has been set at the previously visited MSC. When the new MSC receives the registration message from the mobile station, it proceeds to notify the HLR as set forth in FIGURE 18. The HLR will have stored information contained therein that the presently visited network is not OTAPA capable. Thus the OTAPA pending flag is stored in the HLR and the OTAF address is set and the registration notification reply is returned to the MSC. In the situation presented in the present figure, the system awaits the return of the mobile station to an OTAPA capable system before again attempting the OTAPA update process.

The time sequence diagram of FIGURE 20 addresses the situation where the MSC makes a determination in accordance with pre-established parameters that the mobile station is no longer available to the MSC. This may be a timeout or may be due to other system defined parameters. In any event, the MSC sends a message to the HLR for the mobile station involved that the MSC is clearing its flags because of a determination that the mobile station is inactive. The messages sent from a MSC to the HLR causes an OTAPA pending flag to be set at the HLR and the OTAF address is stored as well. A message is then returned to the MSC indicating that the HLR has properly received the mobile station inactive message and accompanying data.

The time sequence diagram of FIGURE 21 addresses the situation where the HLR does not have location information of the mobile that the HLR believes is correct. This typically happens when the mobile station has not registered with a network over a long period of time. In such a situation an OTAPA pending flag is the set in the HLR and the OTAF address is stored so that when the mobile station next accesses the network, the OTAF can be notified to again commence the OTAPA process.

The time sequence diagram of FIGURE 22 is very similar to that of FIGURE 21. As set forth in FIGURE 22 there are reasons for returning a postponed message from the HLR to the OTAF in addition to those set forth in FIGURE 21. Although obvious to one skilled in the art, FIGURE 22 also uses a slightly different data nomenclature within the short message service request.

The time sequence diagram of FIGURE 23 may be considered a continuation of the diagram of either FIGURES 21 or 22. Since the OTAPA pending flag has been set in the HLR as illustrated in each of the FIGURES 20-22, this will be observed to be the same situation as initially set forth in FIGURE 23. Although the storage of the OTAF address is not specifically set forth in the presentation of FIGURE 23, it is implied. When the visited MSC receives a registration request from the mobile station, a registration notification is sent from the MSC to the HLR if the visited MSC network is OTAPA capable. The OTAPA pending flag is cleared and a reply is returned to the MSC with the OTAF address and an OTAPA pending flag may be set at this time in the MSC. The OTAF is notified and a reply is returned to the MSC that OTAF has received the notification. The OTAF entity returns a protocol capability request to the MSC and the process proceeds as shown in the previously discussed figures such as those discussed in FIGURES 6 through 10. In other words, there

will be a network validation, a service programming lock procedure and the update before clearing the various flags and registers.

The time sequence diagram of FIGURE 24, addresses the situation where an OTAPA procedure has been attempted and a determination made that the mobile station is unavailable. As illustrated, the MSC has an OTAPA flag pending set and the OTAF address has been stored. It is now shown that an OTASP call is received for a user-initiated updating of the mobile station. Such a situation may occur due to the receipt by the user of a mailed or otherwise delivered communication that the mobile station needs to be updated to correctly operate in accordance with the user's desires. When an MSC receives an OTASP call with the OTAPA pending flag set, it delivers a message to the CSC of the mobile station. A set of messages listed as dialogue between the mobile station user and the CSC operator is set forth. As is illustrated at the bottom of this figure, the OTAF then sends a request to the MSC to clear the OTAPA pending flag. A reply to this request is sent from the MSC to the OTAF entity.

The time sequence diagram of FIGURE 25 provides an alternate approach to the situation addressed in FIGURE 24. The process as illustrated in FIGURE 25 has the HLR return data to the OTAF which then proceeds to communicate directly with the MSC. When the MSC determines that the mobile station is unavailable, it stores the OTAF address, sets an OTAPA pending flag and returns a "postponed" message to OTAF. When a user initiated OTASP call is received by the MSC, normal user initiated OTASP procedures are followed as set forth in previous figures. Upon completion of the OTASP process, the MSC clears the OTAF address and clears the OTAPA pending flag. This action assumes that as part of OTASP programming, the programming that would have been performed by an OTAPA session was accomplished.

The time sequence diagram of FIGURE 26 addresses the situation where the HLR knows that the mobile station is in a network wherein it is inappropriate to do an OTAPA process. It may be that the visited network is not "trustworthy" or it may be that the visited system merely is not OTAPA capable. In any event the HLR sends a denied message to the OTAF entity. Although not shown, the HLR may set the OTAPA pending flag, store the OTAF address and return a postponement message to the OTAF entity. Such an alternate action will ensure that the OTAPA process will be performed at a later time when the mobile

station is in an appropriate visited network or returns to the home network. This alternate action is shown in FIGURES 21 and 22.

The time sequence diagram of FIGURE 27 is very similar to that of FIGURE 26 in a comparative manner similar to that of FIGURES 22 and 21. FIGURE 27 uses slightly different nomenclature in defining the data used in the short message service request and further lists additional reasons for why the HLR would return a "denied" request to the OTAF. As presented, the mobile station location may not be available, the mobile station may be in a network not capable of OTAPA or the mobile station may be in an area where OTAPA is not authorized.

The time sequence diagram of FIGURE 28 is a generalization of the actions taken in many previous figures such as Figures 21, 22, 26 and 27. Further the generalized approach could be used as a modification of other Figures such as 16 and 25 where the flag may advantageously be set in the HLR rather than in the MSC. As shown, once the MS becomes available after the flag is set, a notification is returned to the OTAF and an appropriate protocol capability request is issued by the OTAF. The OTAPA process is performed and upon completion of the process, the flag is cleared as shown in previous figures.

Note that the invention describes terms such as comparing, validating, selecting or other terms that could be associated with a human operator. However, for at least a number of the operations described herein which form part of the present invention, no action by a human operator is desirable. The operations described are, in large part, machine operations processing electrical signals to generate other electrical signals.

In summary, the present invention permits a service operator or service provider to initiate the updating of a mobile subscribers terminal in an unobtrusive manner while still providing the security necessary to prevent unauthorized updating by other network providers or hackers. This process is designated herein as OTAPA. The updating may be initiated by sending a page to the mobile terminal or station. The page message includes a service option indication that lets the mobile station know that an updating procedure is to be performed. The mobile station also knows from the service option indication that it should not ring the user of the station. Thus the mobile terminal user is not unnecessarily disturbed.

Once the mobile station has been located, the remaining messages can be transmitted in a variety of formats depending upon the system used to complete the updating process and a general page broadcast may also be used. However, using a broadcast method is undesirable

from a security standpoint and using the paging access channel typically will overburden this system resource. Many systems, such as CDMA, permit the multiplexing of signaling and voice messages on a given traffic channel. Thus, the preferred mode is to use the traffic channel whether or not the mobile station user is presently participating in a phone communication.

Subsequent to being notified by the network that an update procedure is to be initiated, the mobile station initiates a network validation scheme referred to herein as SPASM. SPASM uses portions of a previously used authentication scheme. In the SPASM process, the mobile station generates a random number which is combined with other internally stored information to produce a unique authorization word. The home network has a copy of this stored information. Typically this is stored in the AC and thus the network generates the same unique authorization word after receiving a copy of the random number generated within the mobile station. This network generated authorization word is returned to the mobile station where it is compared. Upon successful comparison, the mobile station performs a service lock process (actually an unlock process) and then performs the OTAPA update procedure.

While the SPASM process is not mandatory as a prerequisite to performing the OTAPA process, service providers in general want the security afforded the service provider by this validation process.

The concept presented in this document includes the use of flags set in the network when the OTAPA process cannot be completed for any of various reasons. These reasons include the situation where the mobile station cannot be located or is located in a visited network and it is impractical or undesirable to update the mobile station in that specific visited network. This flag may be located in the MSC or the HLR and it may need to be transferred to another MSC or to the HLR in certain situations.

It will thus be apparent that the present invention may be implemented in many different forms or embodiments in accordance with the desires of the service provider. In other words, some of the alternate embodiment's or portions of the overall concept are optional and may be practiced in various manners such as performing the OTAPA process using paging or traffic channels.

It should be noted that the description provided herein is but several examples of an implementation of the present invention. It should be noted that many additional implementations may also be utilized to realize the present invention.

While there have been described herein the principles of the invention, it is to be clearly understood to those skilled in the art that this description is made by way of example only and not as a limitation to the scope of the invention. Accordingly, it is intended, by the appended claims, to cover all modifications of the invention which fall within the true spirit and scope of the invention.

APPENDIX A

Terms and Definitions

AC. See Authentication Center.

Activation Code. A user-entered combination of a specified Feature Code (*FC) and defined group of at least two dialed digits (System Selection Code) that specify the user selection of a Band and a Block operated by the selected service provider.

A-key. A secret, 64-bit pattern stored in the mobile station and HLR/AC. It is used to generate/update the mobile stations Shared Secret Data.

Analog Voice Channel. An analog channel on which a voice conversation occurs and on which brief digital messages may be sent from a base station to a mobile station or from a mobile station to a base station.

Authentication. A procedure used by a base station to validate a mobile stations identity.

Authentication Center (AC). An entity that manages the authentication information related to the mobile station.

Base Station. A station in the Domestic Public Cellular Radio Telecommunications Service, other than a mobile station, used for communicating with mobile stations. Depending upon the context, the term base station may refer to a cell, a sector within a cell, an MSC, or other part of the cellular system. See also MSC.

CRC. See Cyclic Redundancy Code.

Cyclic Redundancy Code (CRC). A class of linear error detecting codes which generate parity check bits by finding the remainder of a polynomial division.

Electronic Serial Number (ESN). A 32-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment.

ESN. See Electronic Serial Number.

Forward CDMA Channel. A CDMA Channel from a base station to mobile stations. The Forward CDMA Channel contains one or more code channels that are transmitted on a CDMA frequency assignment using a particular pilot PN offset. The code channels are associated with the Pilot Channel, Sync Channel, Paging Channels, and Traffic Channels. The Forward CDMA Channel always carries a Pilot Channel and may carry up to one Sync Channel, up to seven Paging Channels, and up to 63 Traffic Channels, as long as the total number of channels, including the Pilot Channel, is no greater than 64.

Forward Analog Voice Channel (FVC). An analog voice channel used from a base station to a mobile station.

Forward Traffic Channel. A code channel used to transport user and signaling traffic from the base station to the mobile station.

HLR. See Home Location Register.

Home Location Register (HLR). The location register to which a MIN/IMSI is assigned for record purposes such as subscriber information.

Home System. The cellular system in which the mobile station subscribes for service.

IMSI. See International Mobile Station Identity.

IMSI_M. MIN based IMSI using the lower 10-digits to store the MIN.

IMSI_T. IMSI not associated with MIN. Could be 15-digits or less.

International Mobile Station Identity (IMSI). A method of identifying stations in the land mobile service as specified in CCITT Recommendation E.212.

Long Code Mask. A 42-bit binary number that creates the unique identity of the long code. See also Public Long Code, Private Long Code, Public Long Code Mask, and Private Long Code Mask.

LSB. Least significant bit.

MCC. See Mobile Country Code.

MIN. See Mobile Identification Number.

MNC. See Mobile Network Code.

Mobile Country Code (MCC). A part of the E.212 IMSI identifying the home country. See CCITT Recommendation E.212.

MOBILE DIRECTORY NUMBER. A dialable directory number which is not necessarily the same as the mobile stations air interface identification, i.e., MIN, IMSI_M or IMSI_T.

Mobile Network Code (MNC). A part of the E.212 IMSI identifying the home network within the home country. See CCITT Recommendation E.212.

Mobile Station. A station in the Domestic Public Cellular Radio Telecommunications Service intended to be used while in motion or during halts at unspecified points. Mobile stations include portable units (e.g., hand-held personal units) and units installed in vehicles.

Mobile Identification Number (MIN). The 34-bit number that is a digital representation of the 10-digit number assigned to a mobile station.

Mobile Station Originated Call. A call originating from a mobile station.

Mobile Station Terminated Call. A call received by a mobile station (not to be confused with a disconnect or call release).

Mobile Subscriber or User. The person or entity using a mobile station.

Mobile Switching Center (MSC). A configuration of equipment that provides wireless radiotelephone service. Also called the Mobile Telephone Switching Office (MTSO).

MSB. Most significant bit.

MSC. See Mobile Switching Center.

NAM. See Number Assignment Module.

Network. A network is a subset of a cellular system, such as an area-wide cellular network, a private group of base stations, or a group of base stations set up to handle a special requirement. A network can be as small or as large as needed, as long as it is fully contained within a system. See also System.

Network Identification (NID). A number that uniquely identifies a network within a wireless system. See also System Identification.

NID. See Network Identification.

Number Assignment Module (NAM). A set of MIN/IMSI-related parameters stored in the mobile station.

OTAF. See Over-the-Air Functional Entity.

Over-the-Air Functional Entity (OTAF). A configuration of network equipment that controls OTASP functionality and messaging protocol.

OTAPA. See Over-the-Air Parameter Administration.

Over-the-Air Parameter Administration (OTAPA). Network initiated OTASP process of provisioning mobile station operational parameters over the air interface.

OTASP. See Over-the-Air Service Provisioning.

Over-the-Air Service Provisioning (OTASP). A process of provisioning mobile station operational parameters over the air interface.

Parity Check Bits. Bits added to a sequence of information bits to provide error detection, correction, or both.

Private Long Code. The long code characterized by the private long code mask.

Private Long Code Mask. The long code mask used to form the private long code. See also Public Long Code Mask and Long Code.

Public Long Code. The long code characterized by the public long code mask.

Public Long Code Mask. The long code mask used to form the public long code. The mask contains the ESN of the mobile station. See also Private Long Code Mask.

Release. A process that the mobile station and base station use to inform each other of call disconnect.

Reverse CDMA Channel. The CDMA Channel from the mobile station to the base station. From the base stations perspective, the Reverse CDMA Channel is the sum of all mobile station transmissions on a CDMA frequency assignment.

Roamer. A mobile station operating in a cellular system (or network) other than the one from which service was subscribed. See also Foreign NID Roamer and Foreign SID Roamer.

Service Option. A service capability of the system. Service options may be applications such as voice, data, or facsimile. See TSB58A, "Administration of Parameter Value Assignments for TIA/EIA Spread Spectrum Standards."

Service Programming Lock (SPL). A protection provided for preventing the over-the-air provisioning of certain mobile station parameters by unauthorized network entity by way of verifying the Service Programming Code (SPC).

Shared Secret Data (SSD). A 128-bit pattern stored in the mobile station (in semi-permanent memory) and known by the base station. SSD is a concatenation of two 64-bit subsets: SSD_A, which is used to support the authentication procedures, and SSD_B, which serves as one of the inputs to the process generating the encryption mask and private long code.

SID. See System Identification.

SPASM. See Subscriber Parameter Administration Security Mechanism.

Subscriber Parameter Administration Security Mechanism (SPASM). Security mechanism protecting parameters and indicators of active NAM from programming by an unauthorized network entity during the OTAPA session.

SPL. See Service Programming Lock.

SSD. See Shared Secret Data.

SSPR. See System Selection for Preferred Roaming.

System. A system is a cellular telephone service that covers a geographic area such as a city, metropolitan region, county, or group of counties. See also Network.

System Identification (SID). A number uniquely identifying a cellular system.

System Selection Code. A part of the Activation Code that specifies the user selection of a Band and a Block operated by the selected service provider.

System Selection for Preferred Roaming (SSPR).. A feature that enhances the mobile station system acquisition process based on the set of additional parameters stored in the mobile station in the form of a Preferred Roaming List (PR_LIST_{s-p}).

Traffic Channel. A communication path between a mobile station and a base station used for user and signaling traffic. The term Traffic Channel implies a Forward Traffic Channel and Reverse Traffic Channel pair. See also Forward Traffic Channel and Reverse Traffic Channel.

Voice Channel. See Analog Voice Channel.

Voice Privacy. The process by which user voice transmitted over a CDMA Traffic Channel is afforded a modest degree of protection against eavesdropping over the air.

WHAT IS CLAIMED IS:

1. A method for a network to initiate the updating of operational parameters in a mobile station comprising the steps of:

paging a mobile station from the network;

assigning a traffic channel to the mobile station after receiving an acknowledgment of the page;

modifying the mobile station responses to received traffic channel messages in accordance with a parameter updating indicator received from the network; and

updating operational parameters in the mobile station in accordance with data received on the assigned traffic channel.

2. The method of claim 1 comprising in addition:

releasing the traffic channel upon completion of the updating procedure.

3. The method of claim 1 comprising in addition:

comparing a mobile station internally generated signature with a traffic channel received signature where the traffic channel received signature is derived from the home network of the mobile station and where the comparison is performed prior to the updating step.

4. A method of supplying data to be used in a network initiated over the air updating of operational parameters in a wireless communication system mobile station presently using a user communication traffic channel comprising the steps of:

alerting a mobile station to an administrative update;

comparing a mobile station internally generated signature with a traffic channel received signature where the traffic signalling channel received signature is derived from data stored at the home network of the mobile station; and

updating operational parameters in the mobile station in accordance with data received on the assigned traffic signalling channel upon the occurrence of a satisfactory comparison.

5. The method of claim 4 wherein the alerting comprises the use of a unique service option indicator.

6. A wireless communication system comprising:

first means, including stored operational parameters, for providing mobile communications;

mobile switching center means including base station means for communicating with said first means; and

over the air administration means for network initiating the alteration of said operational parameters stored in said first means.

7. The apparatus of claim 6 comprising in addition:

means, comprising part of said first means, for validating the network initiating the alteration of said operational parameters before completing the stored parameter alteration process.

8. A wireless communication system comprising:

mobile station means in contact with at least one base station;

storage means for storing operational parameters comprising a part of said mobile station means;

mobile switching center means in contact with said at least one base station whereby a communication network is formed; and

network initiated means for altering said operational parameters stored in said storage means of said mobile station means in accordance with data transmitted to said mobile station in an over the air administration process.

9. The apparatus of claim 8 comprising in addition:

means, comprising part of said mobile station means, for validating the network, supplying the data transmitted, before completing the stored parameter alteration process.

10. A method of updating operational parameters in a mobile station of a wireless communication network comprising the steps of:

paging a mobile station with a network initiated update request;

correlating a network challenge received by the network from said mobile station with network stored data for validating the network authority to update;

correlating a challenge response from the network with mobile station stored data before accepting update data in said mobile station;

updating operational parameters in said mobile station from network received data; and

returning said mobile station to a status that is other than update status.

11. The method of claim 10 wherein:

the paging includes a service option parameter to set the mobile station in a over the air programming mode.

12. Mobile station means comprising;

over the air functional entity means for receiving programming instructions and data via a traffic signalling channel;

means for validating the identity of a network service provider, attempting to initiate over the air programming of the mobile station, before allowing update data to be stored; and

means for storing over the air received update data.

13. The apparatus of claim 12 wherein:

said means for validating combines stored unique and internally generated data to form a secret word which is matched against a similarly generated secret word formed from home network stored data.

14. A method of alerting a wireless communications network that an attempt to update operational parameters in a mobile station has failed comprising the steps of:

setting a network based over-the-air parameter administration pending flag; and

storing a network based over-the-air functional address for reinitiating the update process.

15. The method of claim 14 wherein:

the over-the-air parameter administration pending flag is set in conjunction with home location register data when the location of an mobile station is not available.

16. The method of claim 14 wherein:

the over-the-air parameter administration pending flag is set in conjunction with MSC based data when an attempted update of an mobile station is not completed.

17. The method of claim 16 comprising the additional step of:

transferring the flag indication to the HLR when an mobile station update is not completed within predetermined parameters.

18. Apparatus for alerting a wireless communications network that an attempt to update operational parameters in a mobile station has failed comprising:

means for setting a network based over the air parameter administration pending flag; and

means for storing a network based over the air functionality address for reinitiating the update process.

19. The apparatus as claimed in claim 18 comprising in addition:

means for setting the over the air parameter administration pending flag in conjunction with home location register data when the location of an mobile station is not available.

20. The apparatus as claimed in claim 18 comprising in addition:

means for setting the over the air parameter administration pending flag in conjunction with MSC based data when an attempted update of an mobile station is not completed.

21. A method of validating a wireless communication network communicating with a mobile station comprising the steps of:

generating a first secret word, within a mobile station, comprising a predetermined combination of a first word stored internal to the mobile station and a second word generated internal to said mobile station;

generating a second secret word, derived from data stored at the home location network, comprising a predetermined combination of said second word obtained from said mobile station and a copy of said first word as obtained from a home location network register;

supplying said second secret word to said mobile station; and

comparing said first and second secret words within said mobile station to validate the communicating network.

22. Apparatus for validating a wireless communication network communicating with a mobile station comprising:

means for generating a first secret word, within a mobile station, comprising a predetermined combination of a first word stored internal to the mobile station and a second word generated internal said mobile station;

means for generating a second secret word, at the home location network, comprising a predetermined combination of said second word received from said mobile station and a copy of said first word as obtained from a home location network register;

means for supplying said second secret word to said mobile station; and

means for comparing said first and second secret words within said mobile station to validate the communicating network.

23. A method of supplying data to be used in a network initiated over the air updating of operational parameters in a wireless communication system mobile station comprising the steps of:

paging a mobile station from the network;

setting an administrative updating indicator in the mobile station in accordance with a received message; and

updating operational parameters in the mobile station in accordance with data received.

24. The method of claim 23 where the setting and updating are performed on the paging channel.

25. The method of claim 23 where the updating is performed on an assigned traffic channel.

26. The method of claim 23 comprising in addition:

comparing a mobile station internally generated secret word with a secret word received from the network where the received secret word is derived from the home network of the mobile station and where the comparison is performed prior to the updating step.

27. A method of supplying data to be used in a network initiated over the air updating of operational parameters in a wireless communication system mobile station comprising the steps of:

paging a mobile station from the network;

supplying a parameter updating indicator to said mobile station; and

updating operational parameters in the mobile station in accordance with data received over the air from the network.

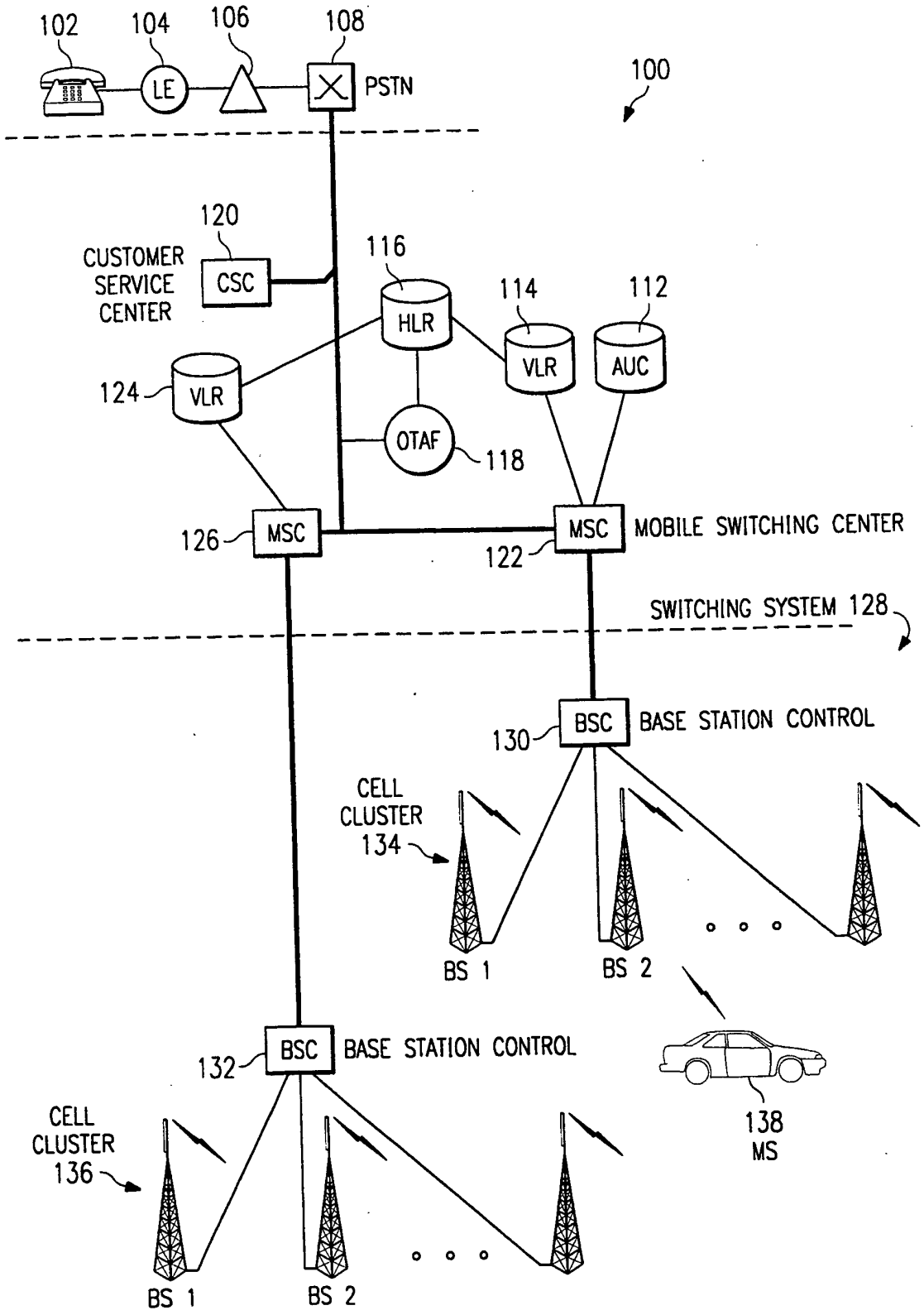

102
104
106
108
LE
PSTN
100
120
CUSTOMER SERVICE CENTER
CSC
116
HLR
114
VLR
112
AUC
124
VLR
OTAF
118
126
MSC
MSC
MOBILE SWITCHING CENTER
122
SWITCHING SYSTEM 128
130
BSC
BASE STATION CONTROL
CELL CLUSTER 134
BS 1
BS 2
132
BSC
BASE STATION CONTROL
CELL CLUSTER 136
BS 1
BS 2
138
MS

FIG. 1

FIG. 2
(PRIOR ART)

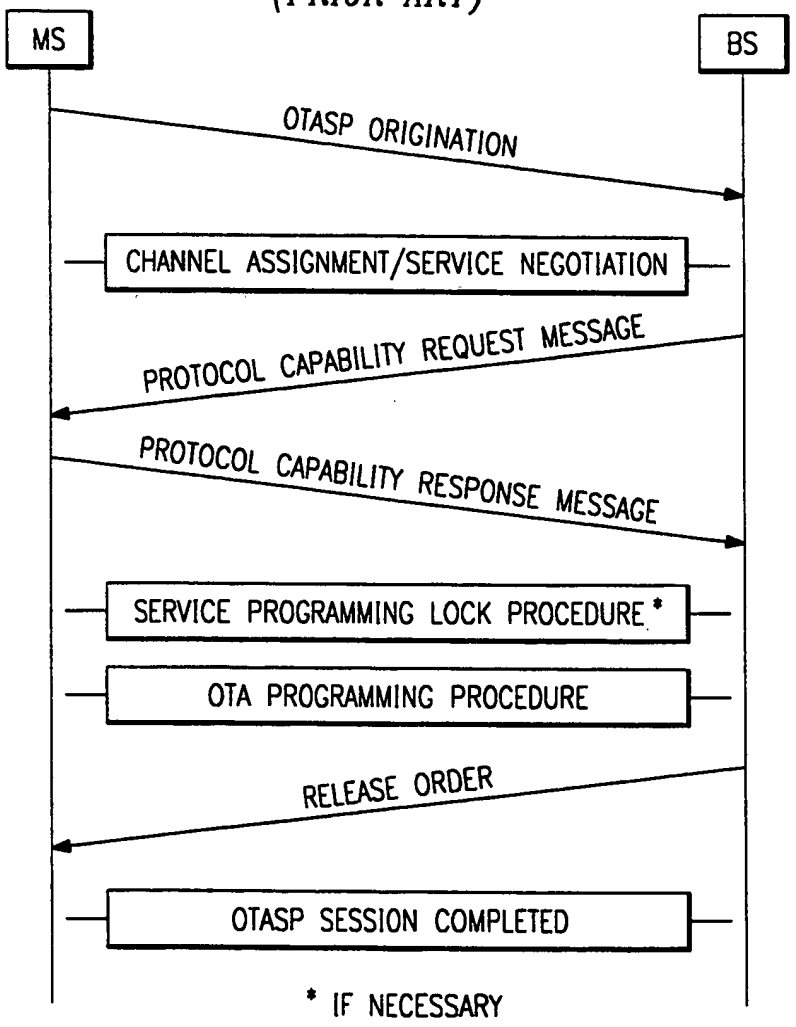


FIG. 3

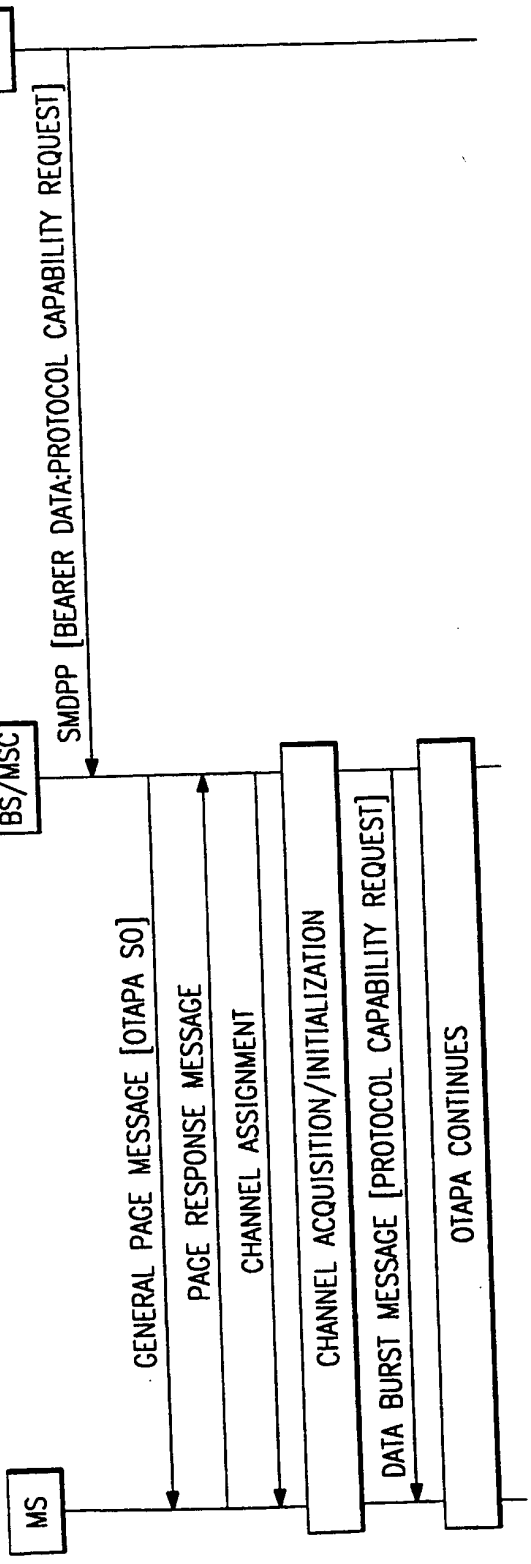
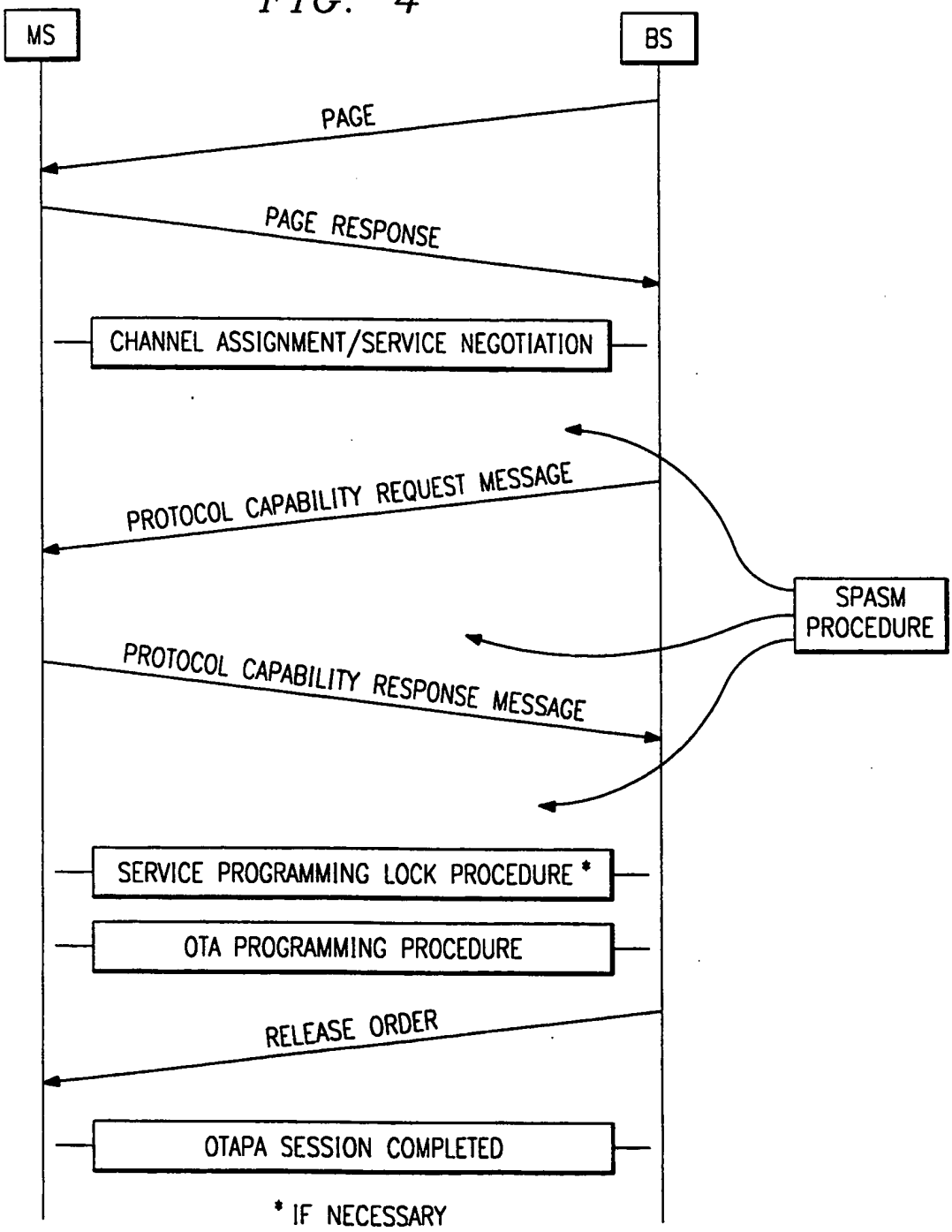


FIG. 4


MS
BS
PAGE
PAGE RESPONSE
CHANNEL ASSIGNMENT/SERVICE NEGOTIATION
PROTOCOL CAPABILITY REQUEST MESSAGE
SPASM PROCEDURE
PROTOCOL CAPABILITY RESPONSE MESSAGE
SERVICE PROGRAMMING LOCK PROCEDURE *
OTA PROGRAMMING PROCEDURE
RELEASE ORDER
OTAPA SESSION COMPLETED
* IF NECESSARY

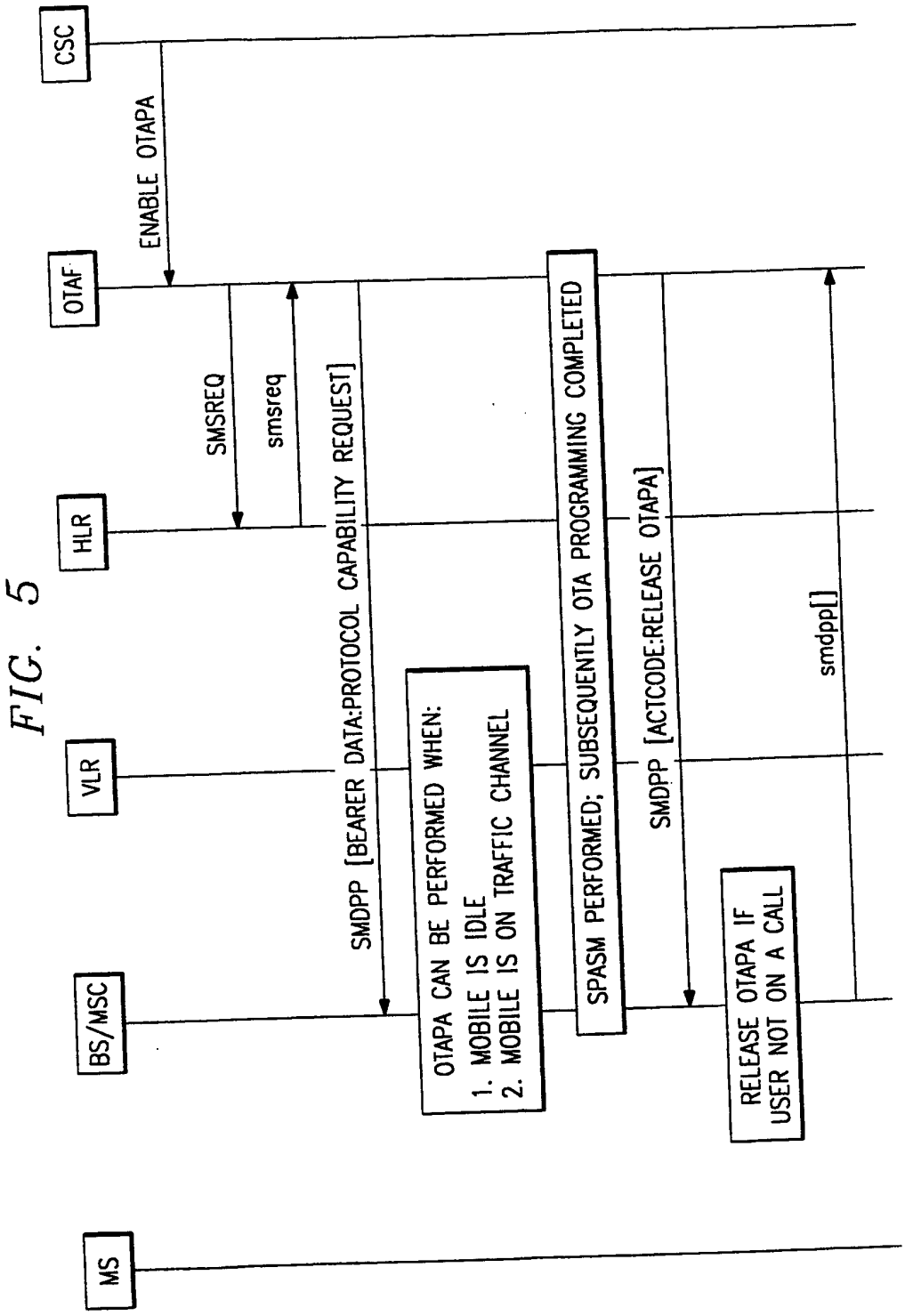

CSC
ENABLE OTAPA
OTAF
SMSREQ
smsreq
HLR
SMDPP [BEARER DATA:PROTOCOL CAPABILITY REQUEST]
VLR
OTAPA CAN BE PERFORMED WHEN:
1. MOBILE IS IDLE
2. MOBILE IS ON TRAFFIC CHANNEL
BS/MSC
SPASM PERFORMED; SUBSEQUENTLY OTA PROGRAMMING COMPLETED
SMDPP [ACTCODE:RELEASE OTAPA]
RELEASE OTAPA IF USER NOT ON A CALL
smdpp[]
MS

FIG. 5

FIG. 6

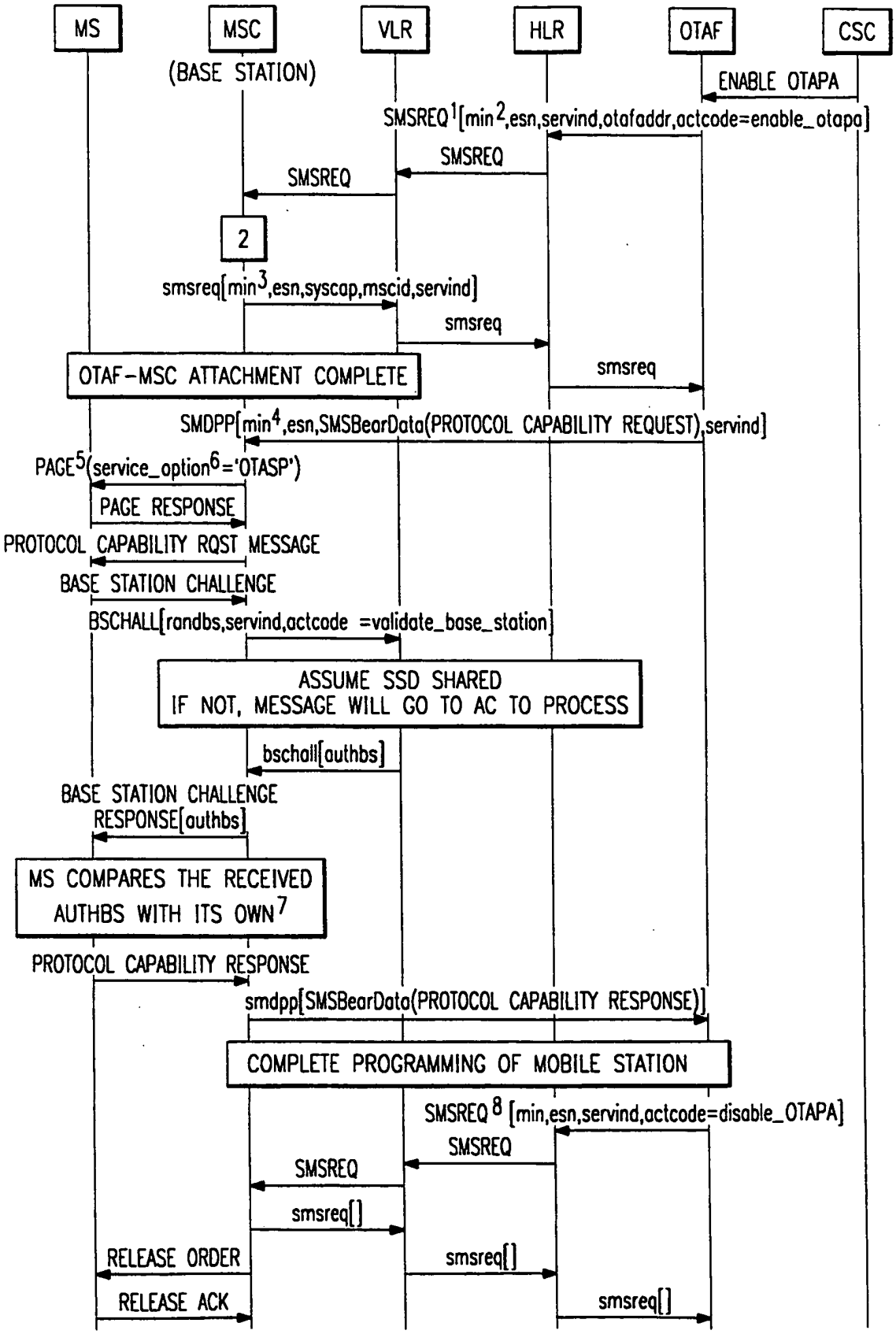
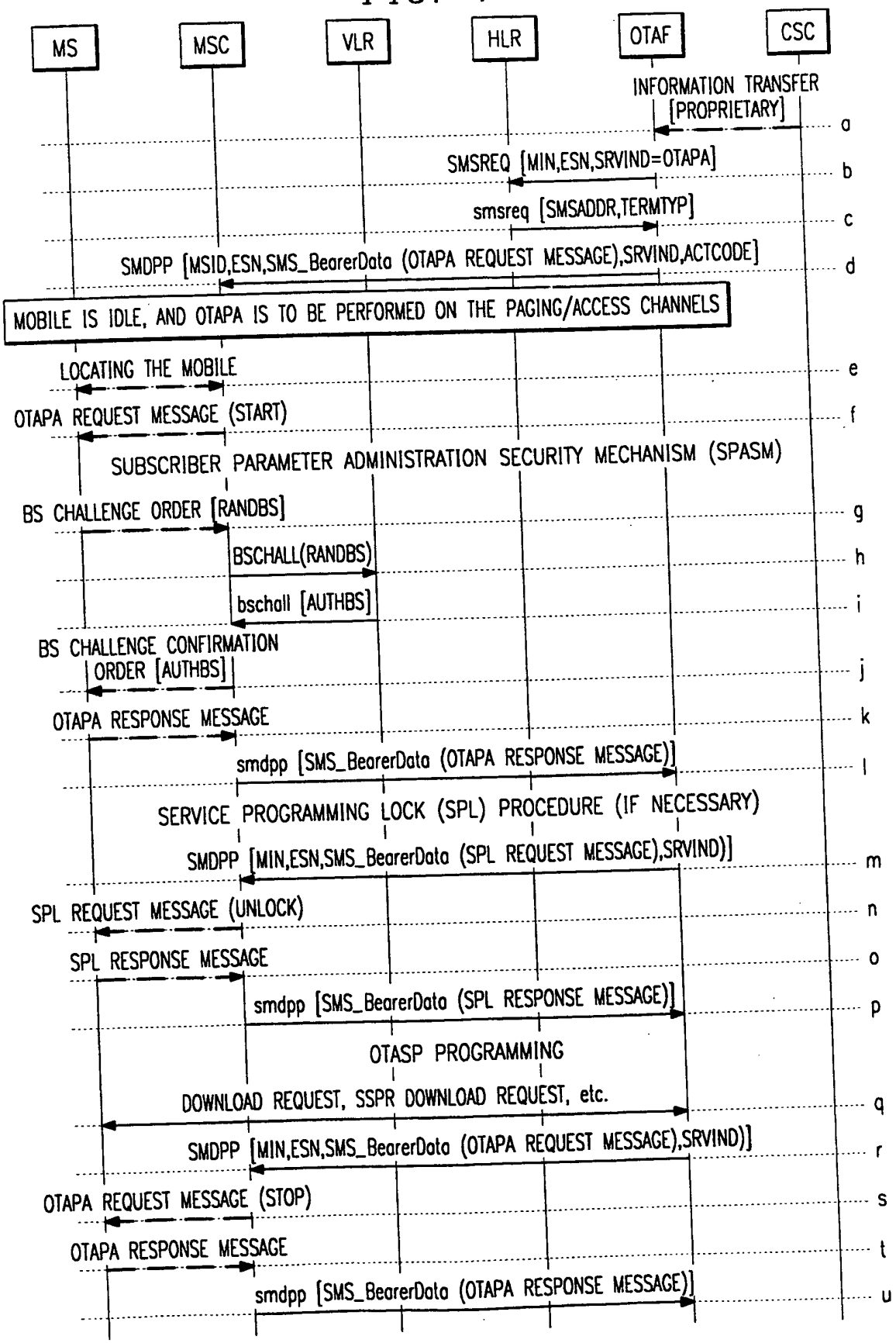

MS
MSC
(BASE STATION)
VLR
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ[1][min[2],esn,servind,otafaddr,actcode=enable_otapa]
SMSREQ
SMSREQ
2
smsreq[min[3],esn,syscap,mscid,servind]
smsreq
OTAF-MSC ATTACHMENT COMPLETE
smsreq
SMDPP[min[4],esn,SMSBearData(PROTOCOL CAPABILITY REQUEST),servind]
PAGE[5](service_option[6]='OTASP')
PAGE RESPONSE
PROTOCOL CAPABILITY RQST MESSAGE
BASE STATION CHALLENGE
BSCHALL[randbs,servind,actcode =validate_base_station]
ASSUME SSD SHARED
IF NOT, MESSAGE WILL GO TO AC TO PROCESS
bschall[authbs]
BASE STATION CHALLENGE
RESPONSE[authbs]
MS COMPARES THE RECEIVED
AUTHBS WITH ITS OWN[7]
PROTOCOL CAPABILITY RESPONSE
smdpp[SMSBearData(PROTOCOL CAPABILITY RESPONSE)]
COMPLETE PROGRAMMING OF MOBILE STATION
SMSREQ[8] [min,esn,servind,actcode=disable_OTAPA]
SMSREQ
SMSREQ
smsreq[]
RELEASE ORDER
smsreq[]
RELEASE ACK
smsreq[]

FIG. 7



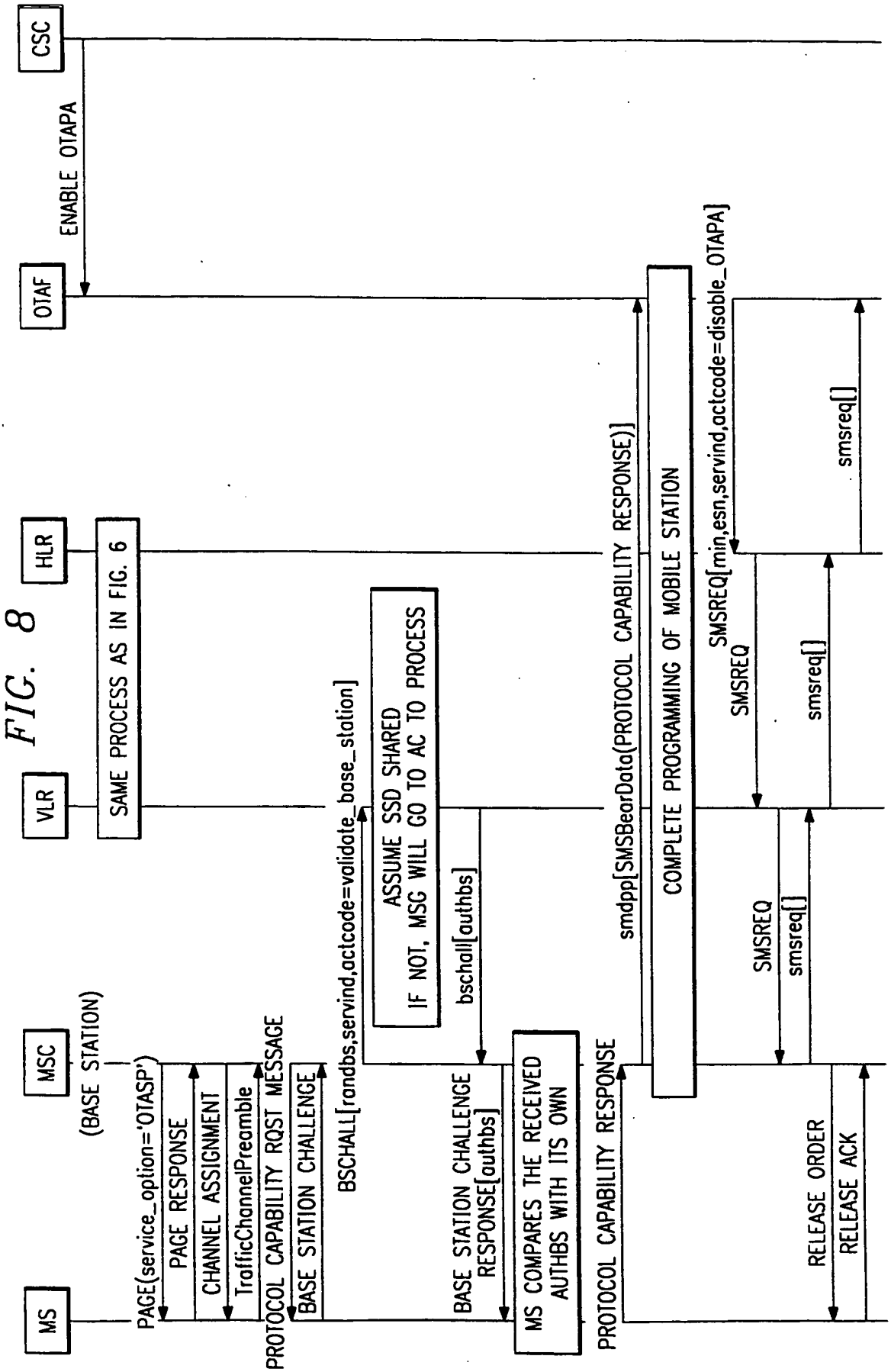

MS
MSC
VLR
HLR
OTAF
CSC
(BASE STATION)
ENABLE OTAPA
SAME PROCESS AS IN FIG. 6
PAGE(service_option='OTASP')
PAGE RESPONSE
CHANNEL ASSIGNMENT
TrafficChannelPreamble
PROTOCOL CAPABILITY RQST MESSAGE
BASE STATION CHALLENGE
BSCHALL[randbs,servind,actcode=validate_base_station]
ASSUME SSD SHARED
IF NOT, MSC WILL GO TO AC TO PROCESS
bschall[authbs]
BASE STATION CHALLENGE
RESPONSE[authbs]
MS COMPARES THE RECEIVED
AUTHBS WITH ITS OWN
PROTOCOL CAPABILITY RESPONSE
smdpp[SMSBearData(PROTOCOL CAPABILITY RESPONSE)]
COMPLETE PROGRAMMING OF MOBILE STATION
SMSREQ[min,esn,servind,actcode=disable_OTAPA]
SMSREQ
smsreq[]
smsreq[]
SMSREQ
smsreq[]
RELEASE ORDER
RELEASE ACK

FIG. 8

FIG. 9

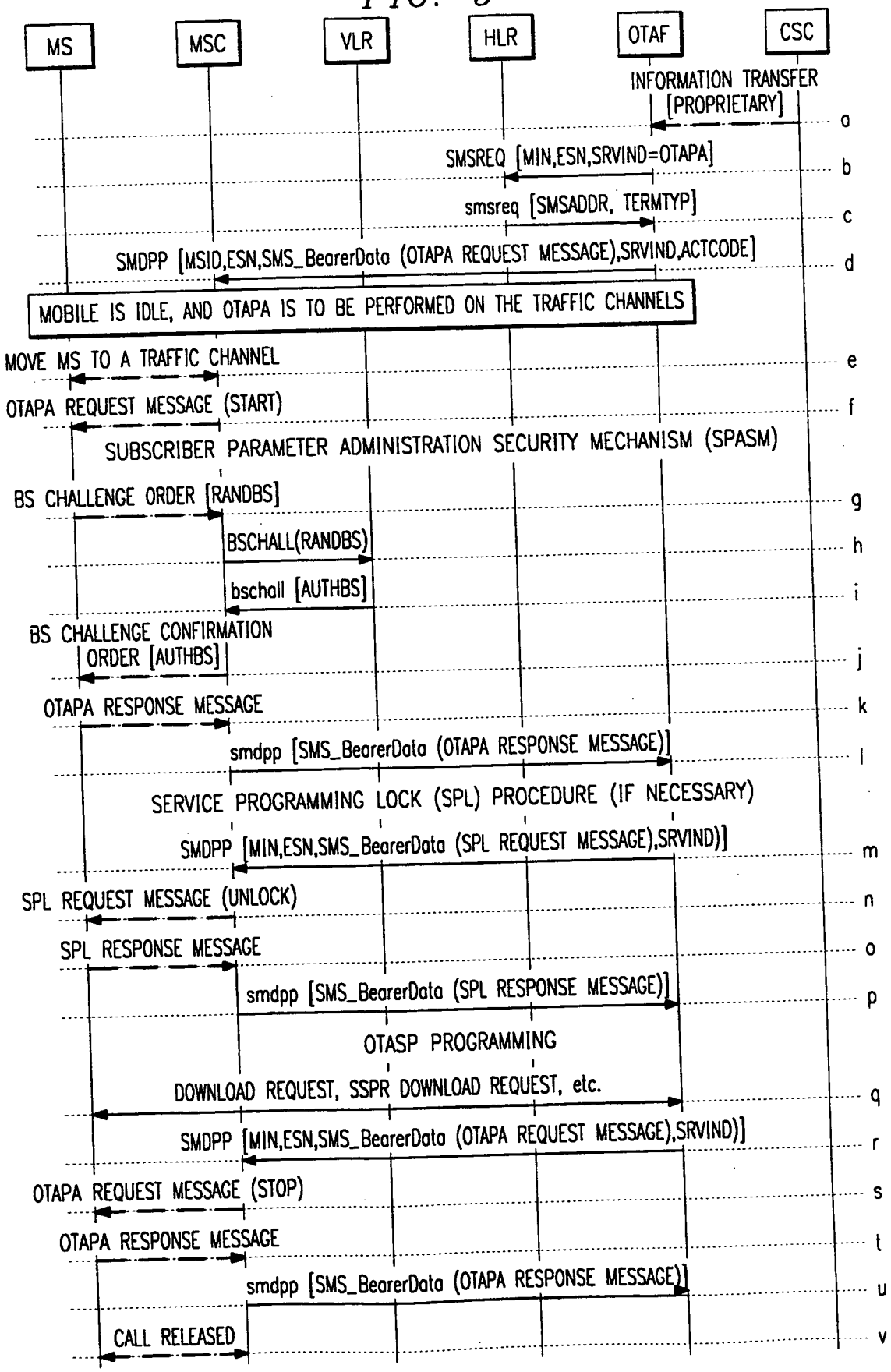


FIG. 10

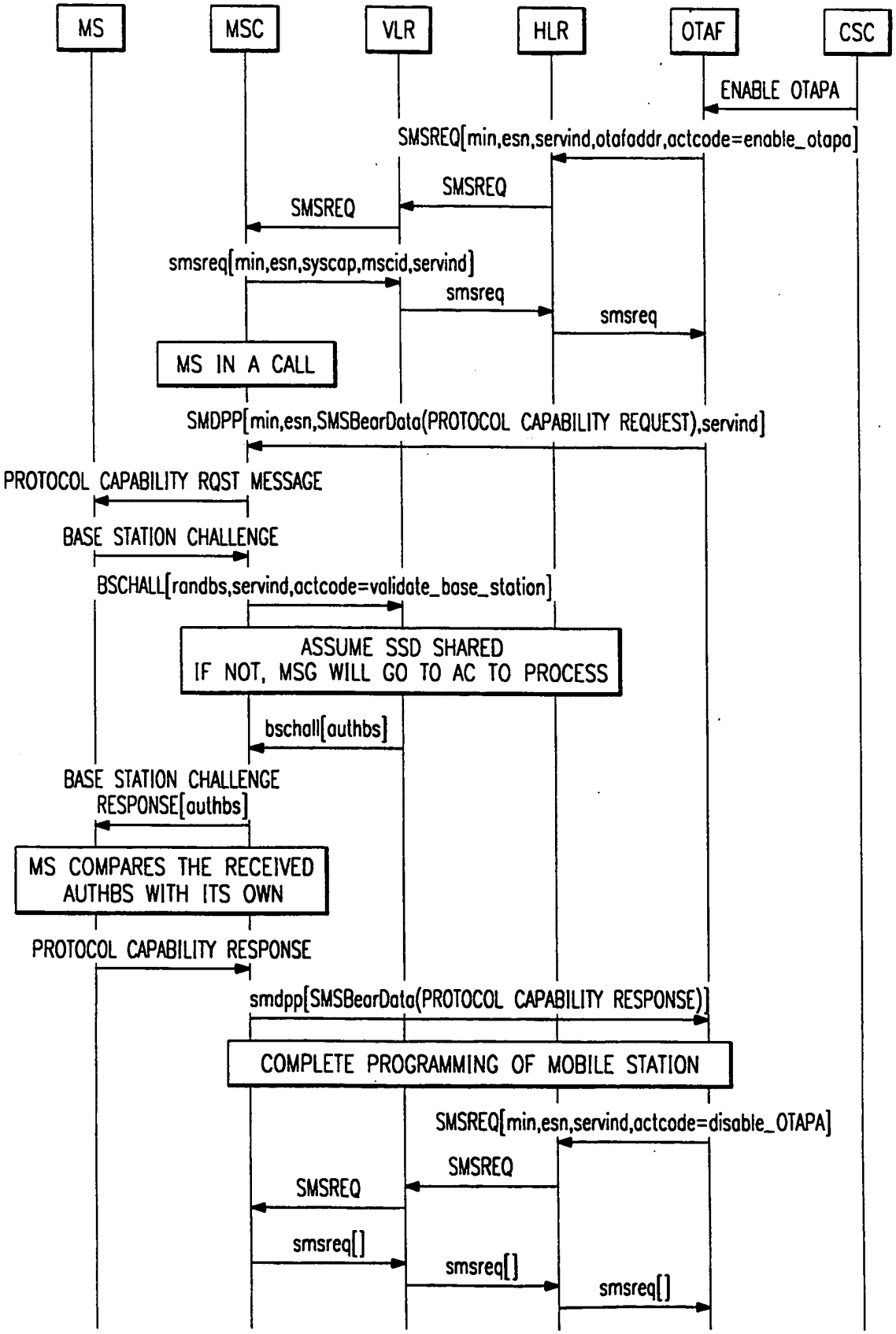

MS
MSC
VLR
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ[min,esn,servind,otafaddr,actcode=enable_otapa]
SMSREQ
SMSREQ
smsreq[min,esn,syscap,mscid,servind]
smsreq
smsreq
MS IN A CALL
SMDPP[min,esn,SMSBearData(PROTOCOL CAPABILITY REQUEST),servind]
PROTOCOL CAPABILITY ROST MESSAGE
BASE STATION CHALLENGE
BSCHALL[randbs,servind,actcode=validate_base_station]
ASSUME SSD SHARED
IF NOT, MSG WILL GO TO AC TO PROCESS
bschall[authbs]
BASE STATION CHALLENGE
RESPONSE[authbs]
MS COMPARES THE RECEIVED
AUTHBS WITH ITS OWN
PROTOCOL CAPABILITY RESPONSE
smdpp[SMSBearData(PROTOCOL CAPABILITY RESPONSE)]
COMPLETE PROGRAMMING OF MOBILE STATION
SMSREQ[min,esn,servind,actcode=disable_OTAPA]
SMSREQ
SMSREQ
smsreq[]
smsreq[]
smsreq[]

FIG. 11

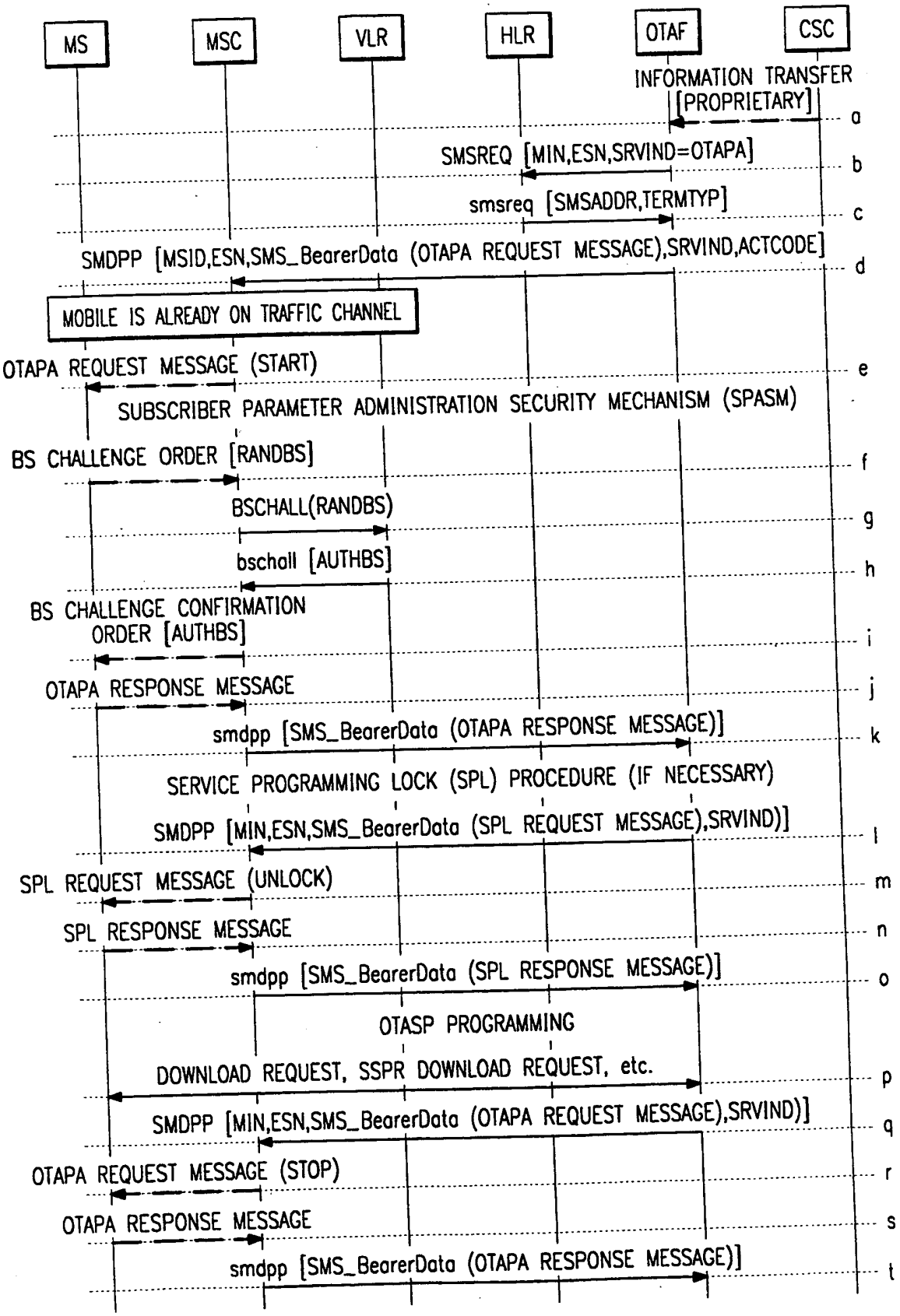

MS
MSC
VLR
HLR
OTAF
CSC
INFORMATION TRANSFER [PROPRIETARY]
a
SMSREQ [MIN,ESN,SRVIND=OTAPA]
b
smsreq [SMSADDR,TERMTYP]
c
SMDPP [MSID,ESN,SMS_BearerData (OTAPA REQUEST MESSAGE),SRVIND,ACTCODE]
d
MOBILE IS ALREADY ON TRAFFIC CHANNEL
OTAPA REQUEST MESSAGE (START)
e
SUBSCRIBER PARAMETER ADMINISTRATION SECURITY MECHANISM (SPASM)
BS CHALLENGE ORDER [RANDBS]
f
BSCHALL(RANDBS)
g
bschall [AUTHBS]
h
BS CHALLENGE CONFIRMATION ORDER [AUTHBS]
i
OTAPA RESPONSE MESSAGE
j
smdpp [SMS_BearerData (OTAPA RESPONSE MESSAGE)]
k
SERVICE PROGRAMMING LOCK (SPL) PROCEDURE (IF NECESSARY)
SMDPP [MIN,ESN,SMS_BearerData (SPL REQUEST MESSAGE),SRVIND)]
l
SPL REQUEST MESSAGE (UNLOCK)
m
SPL RESPONSE MESSAGE
n
smdpp [SMS_BearerData (SPL RESPONSE MESSAGE)]
o
OTASP PROGRAMMING
DOWNLOAD REQUEST, SSPR DOWNLOAD REQUEST, etc.
p
SMDPP [MIN,ESN,SMS_BearerData (OTAPA REQUEST MESSAGE),SRVIND)]
q
OTAPA REQUEST MESSAGE (STOP)
r
OTAPA RESPONSE MESSAGE
s
smdpp [SMS_BearerData (OTAPA RESPONSE MESSAGE)]
t

FIG. 12

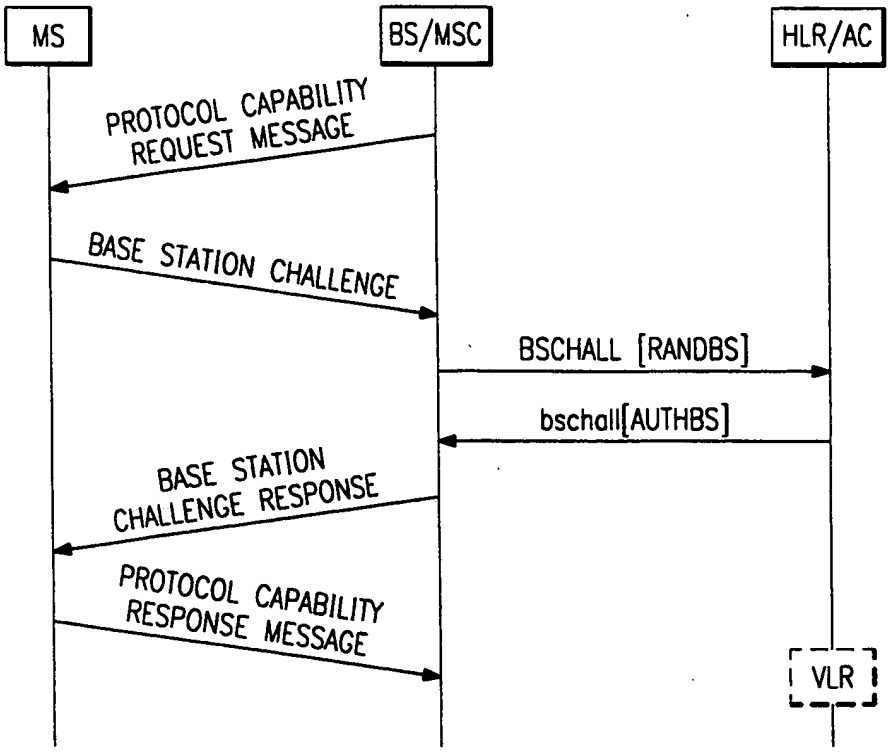

MS
BS/MSC
HLR/AC
PROTOCOL CAPABILITY REQUEST MESSAGE
BASE STATION CHALLENGE
BSCHALL [RANDBS]
bschall[AUTHBS]
BASE STATION CHALLENGE RESPONSE
PROTOCOL CAPABILITY RESPONSE MESSAGE
VLR

FIG. 13

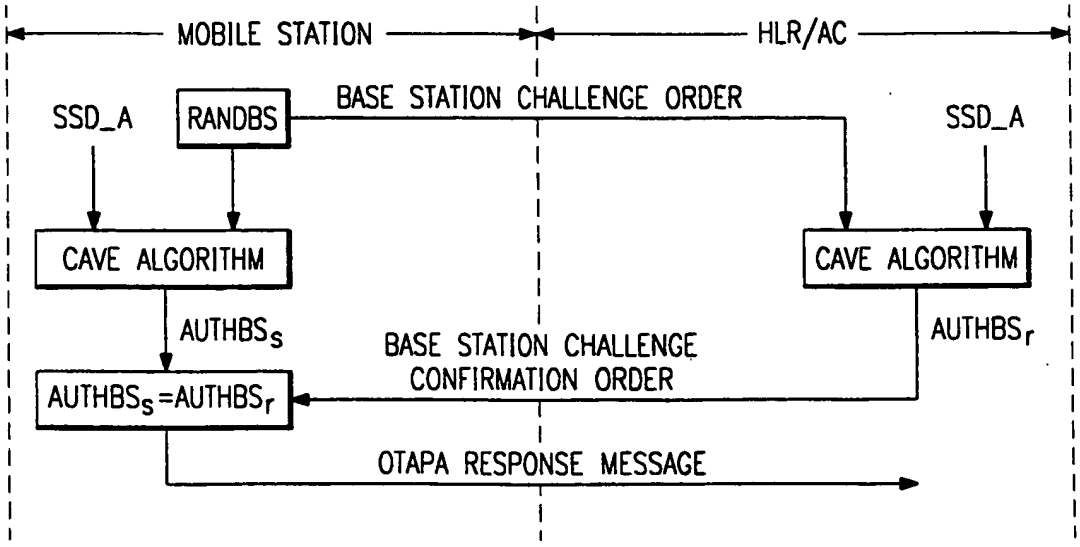

MOBILE STATION
HLR/AC
SSD_A
RANDBS
BASE STATION CHALLENGE ORDER
SSD_A
CAVE ALGORITHM
CAVE ALGORITHM
AUTHBS$_s$
AUTHBS$_r$
BASE STATION CHALLENGE CONFIRMATION ORDER
AUTHBS$_s$=AUTHBS$_r$
OTAPA RESPONSE MESSAGE

FIG. 14

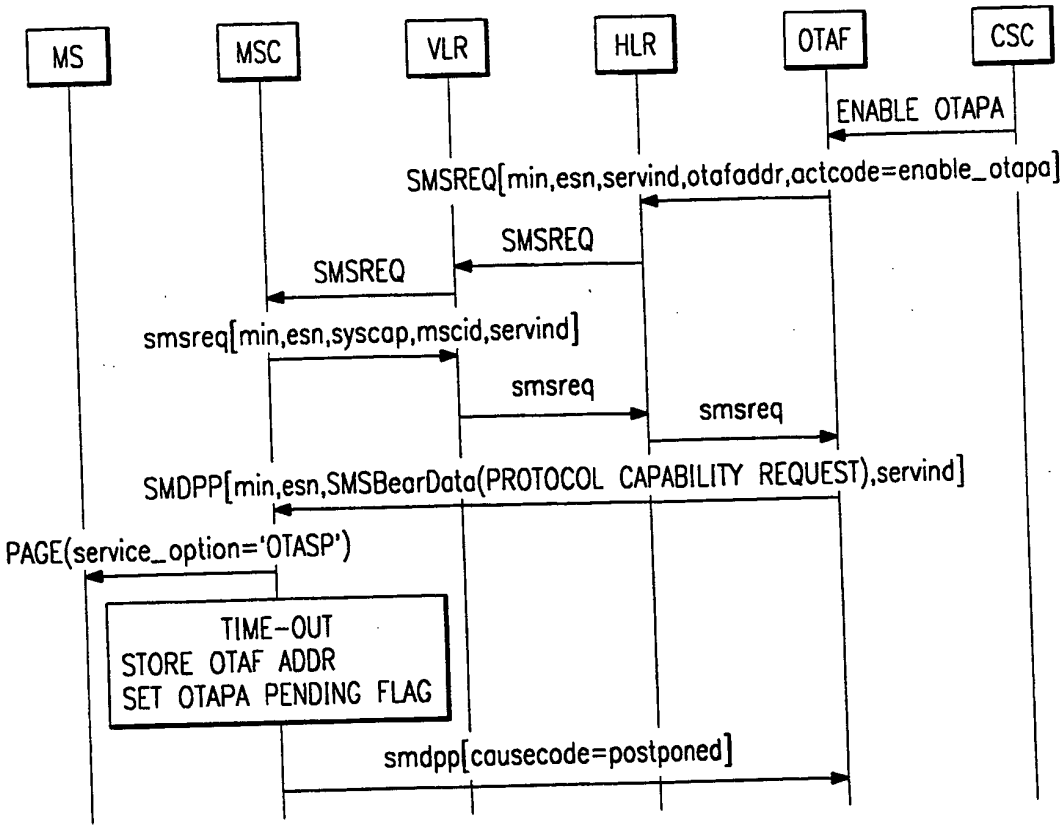

MS
MSC
VLR
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ[min,esn,servind,otafaddr,actcode=enable_otapa]
SMSREQ
SMSREQ
smsreq[min,esn,syscap,mscid,servind]
smsreq
smsreq
SMDPP[min,esn,SMSBearData(PROTOCOL CAPABILITY REQUEST),servind]
PAGE(service_option='OTASP')
TIME-OUT
STORE OTAF ADDR
SET OTAPA PENDING FLAG
smdpp[causecode=postponed]

FIG. 15

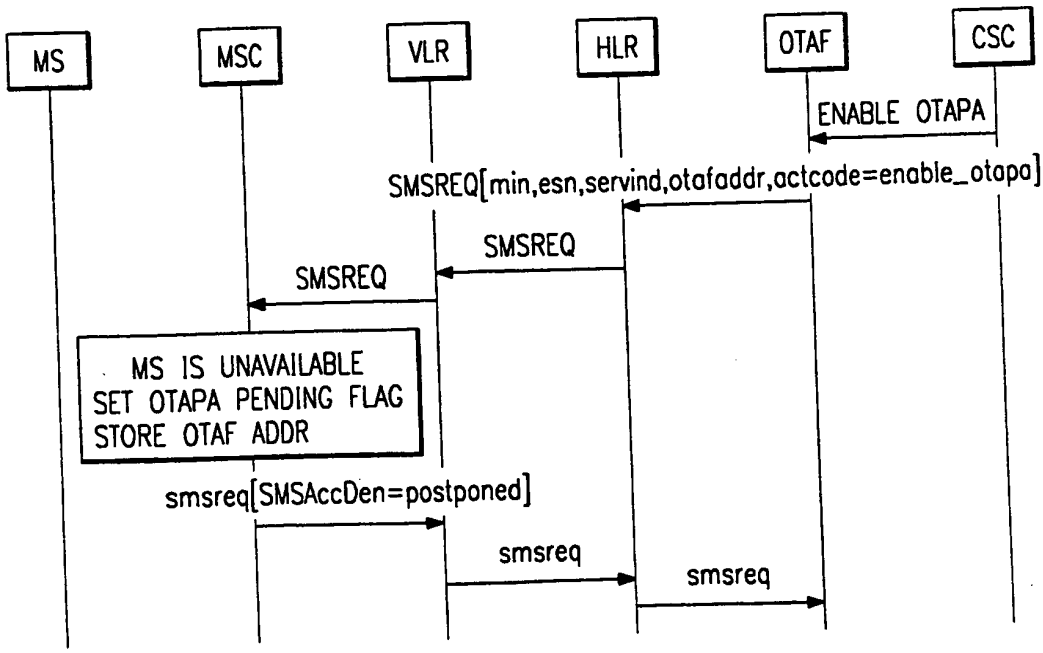

MS
MSC
VLR
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ[min,esn,servind,otafaddr,actcode=enable_otapa]
SMSREQ
SMSREQ
MS IS UNAVAILABLE
SET OTAPA PENDING FLAG
STORE OTAF ADDR
smsreq[SMSAccDen=postponed]
smsreq
smsreq

FIG. 16

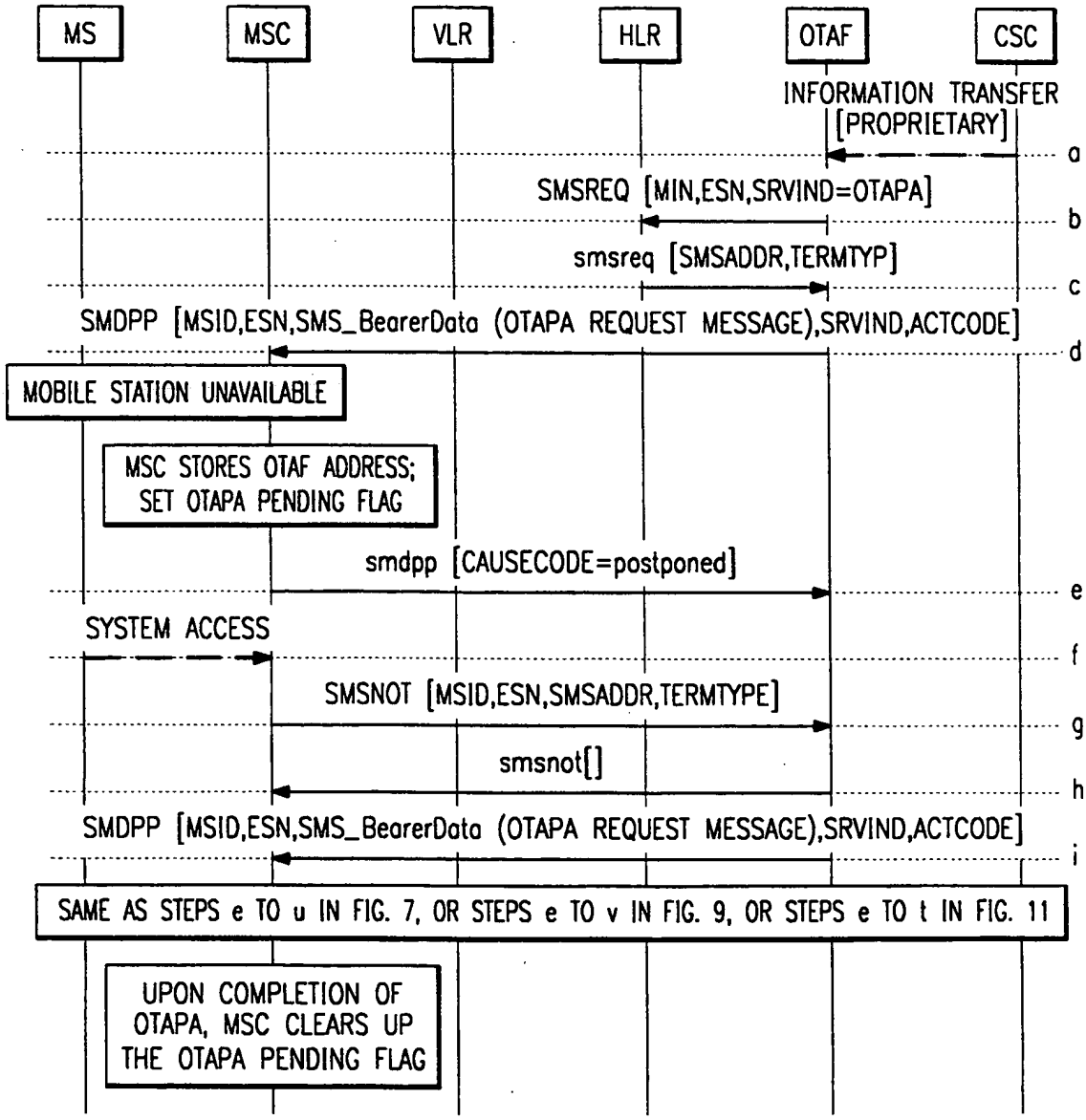
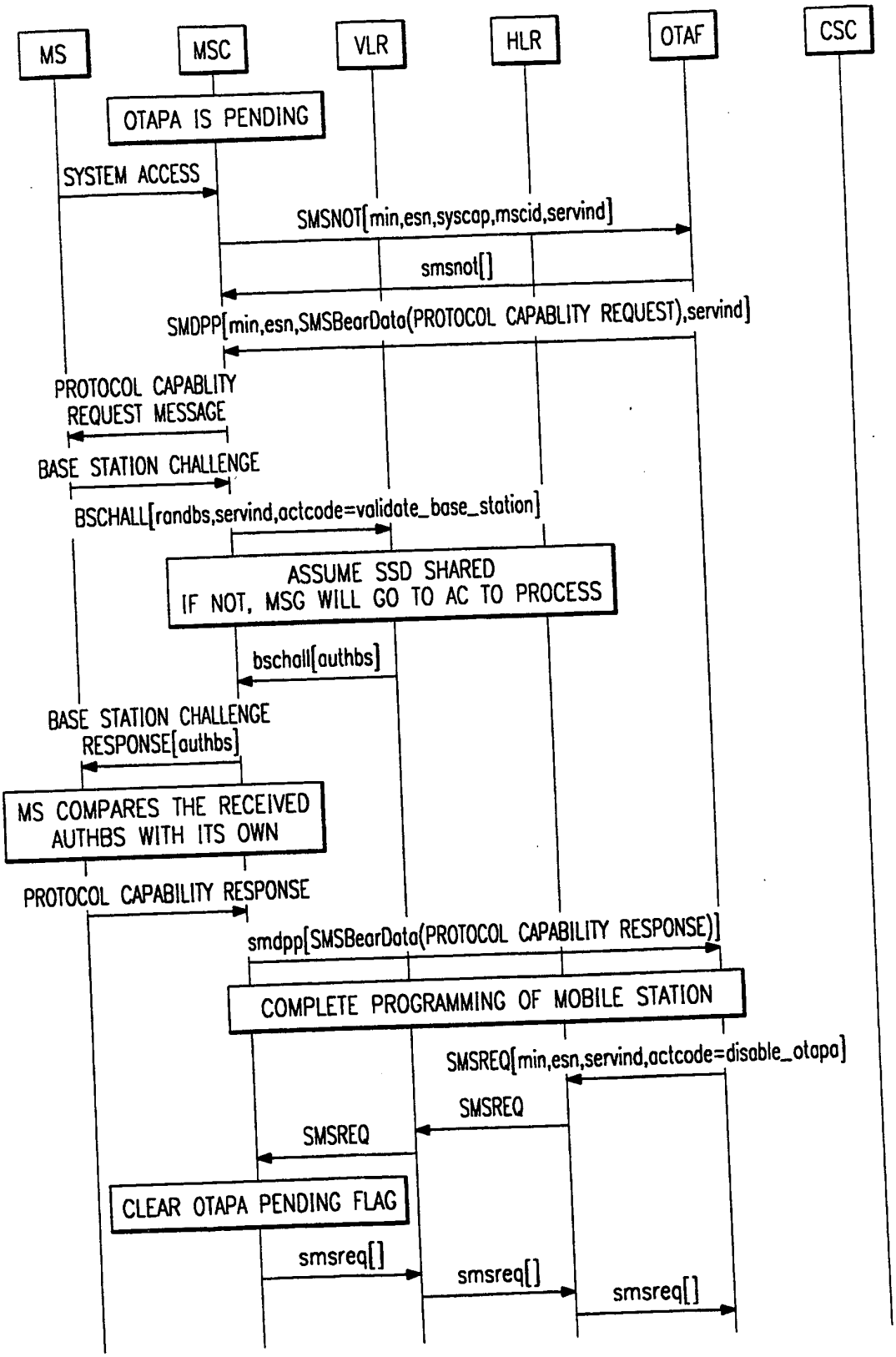

MS
MSC
VLR
HLR
OTAF
CSC
INFORMATION TRANSFER [PROPRIETARY]
a
SMSREQ [MIN,ESN,SRVIND=OTAPA]
b
smsreq [SMSADDR,TERMTYP]
c
SMDPP [MSID,ESN,SMS_BearerData (OTAPA REQUEST MESSAGE),SRVIND,ACTCODE]
d
MOBILE STATION UNAVAILABLE
MSC STORES OTAF ADDRESS; SET OTAPA PENDING FLAG
smdpp [CAUSECODE=postponed]
e
SYSTEM ACCESS
f
SMSNOT [MSID,ESN,SMSADDR,TERMTYPE]
g
smsnot[]
h
SMDPP [MSID,ESN,SMS_BearerData (OTAPA REQUEST MESSAGE),SRVIND,ACTCODE]
i
SAME AS STEPS e TO u IN FIG. 7, OR STEPS e TO v IN FIG. 9, OR STEPS e TO t IN FIG. 11
UPON COMPLETION OF OTAPA, MSC CLEARS UP THE OTAPA PENDING FLAG

FIG. 17


MS
MSC
VLR
HLR
OTAF
CSC
OTAPA IS PENDING
SYSTEM ACCESS
SMSNOT[min,esn,syscap,mscid,servind]
smsnot[]
SMDPP[min,esn,SMSBearData(PROTOCOL CAPABLITY REQUEST),servind]
PROTOCOL CAPABLITY REQUEST MESSAGE
BASE STATION CHALLENGE
BSCHALL[randbs,servind,actcode=validate_base_station]
ASSUME SSD SHARED
IF NOT, MSG WILL GO TO AC TO PROCESS
bschall[authbs]
BASE STATION CHALLENGE RESPONSE[authbs]
MS COMPARES THE RECEIVED AUTHBS WITH ITS OWN
PROTOCOL CAPABILITY RESPONSE
smdpp[SMSBearData(PROTOCOL CAPABILITY RESPONSE)]
COMPLETE PROGRAMMING OF MOBILE STATION
SMSREQ[min,esn,servind,actcode=disable_otapa]
SMSREQ
SMSREQ
CLEAR OTAPA PENDING FLAG
smsreq[]
smsreq[]
smsreq[]

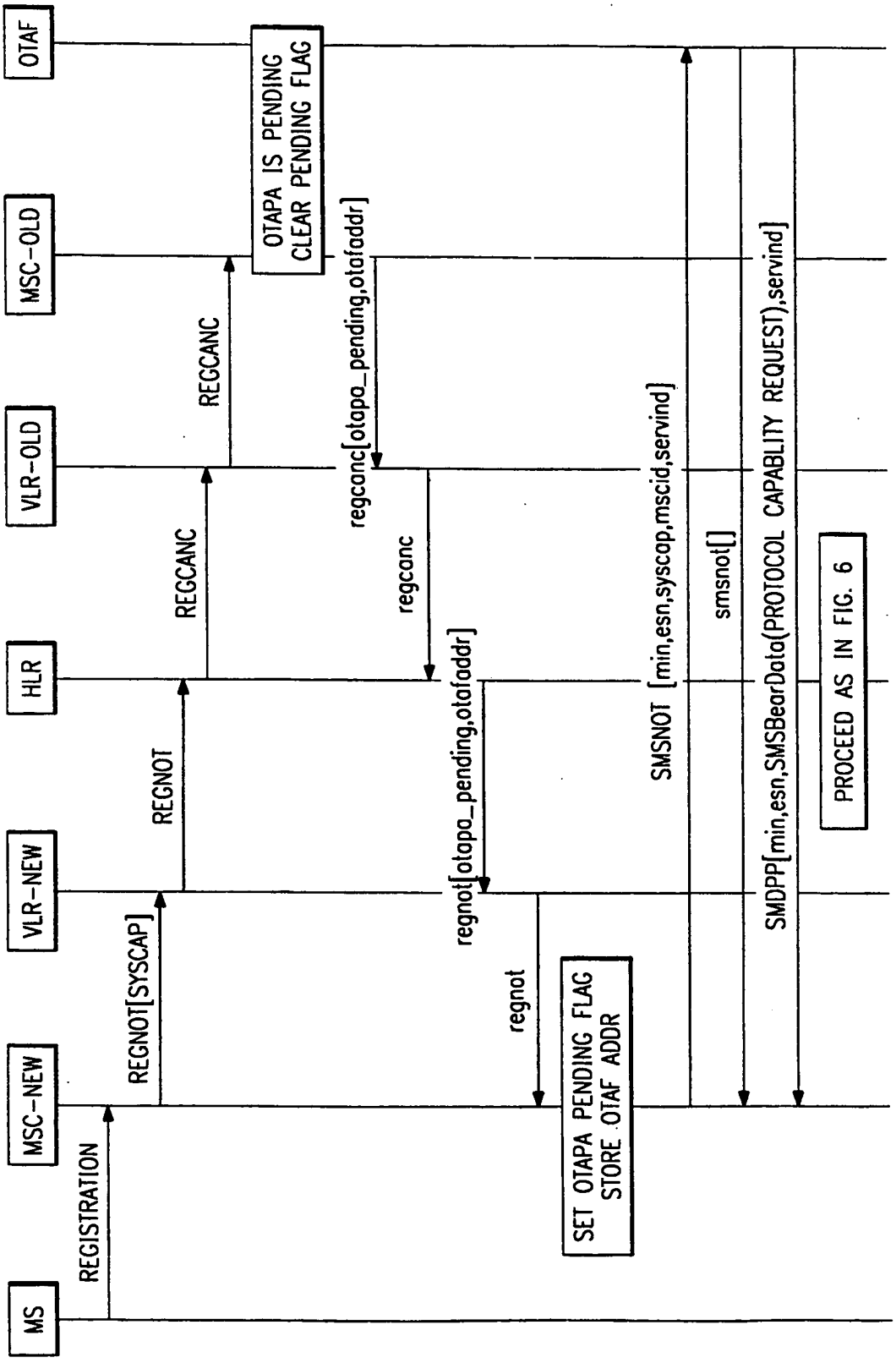

OTAF
MSC-OLD
VLR-OLD
HLR
VLR-NEW
MSC-NEW
MS
OTAPA IS PENDING
CLEAR PENDING FLAG
REGCANC
regcanc[otapa_pending,otafaddr]
REGCANC
regcanc
REGNOT
regnot[otapa_pending,otafaddr]
REGNOT[SYSCAP]
regnot
SET OTAPA PENDING FLAG
STORE OTAF ADDR
REGISTRATION
SMSNOT [min,esn,syscap,mscid,servind]
smsnot[]
SMDPP[min,esn,SMSBearData(PROTOCOL CAPABLITY REQUEST),servind]
PROCEED AS IN FIG. 6

FIG. 18

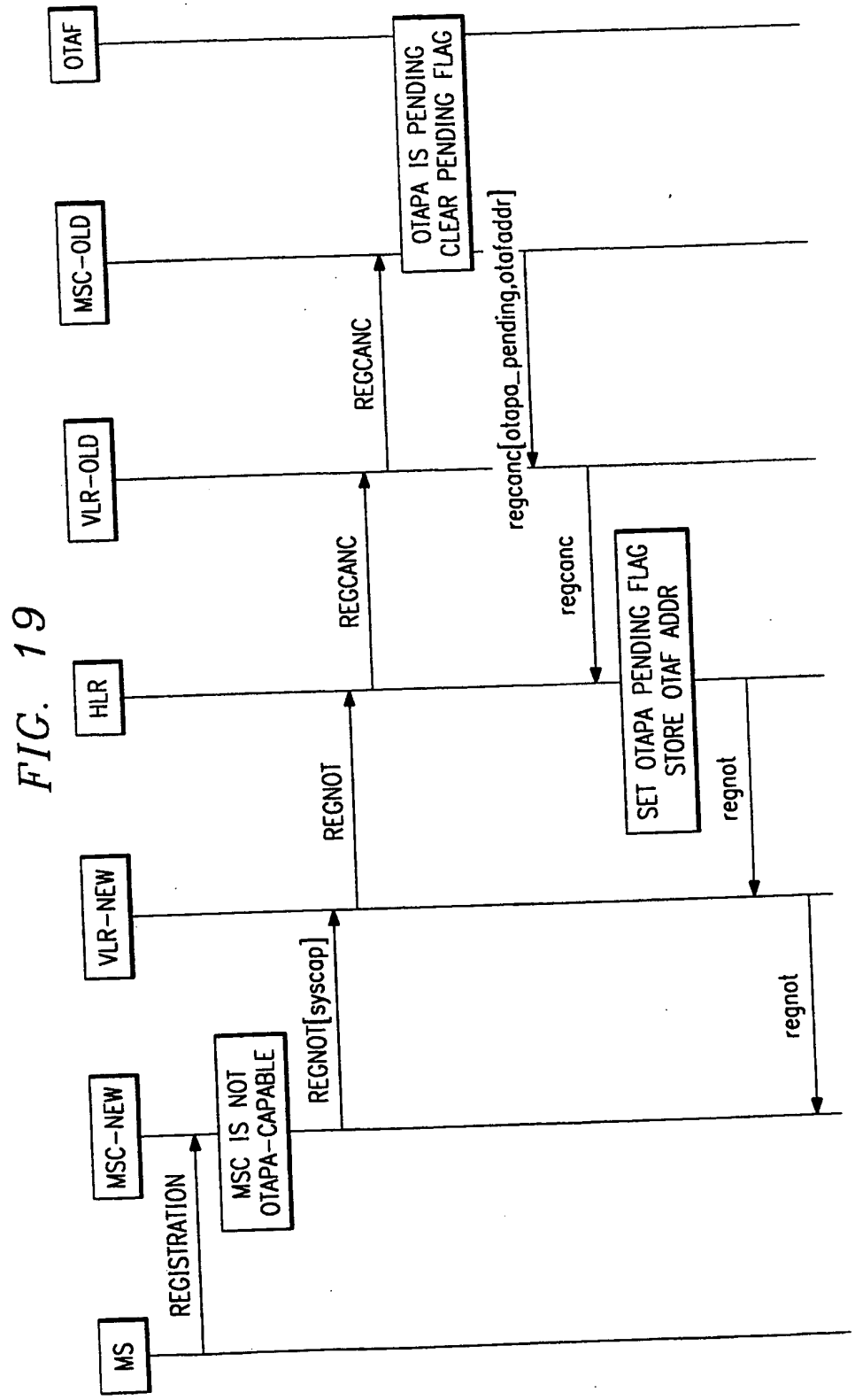

OTAF
MSC-OLD
VLR-OLD
HLR
VLR-NEW
MSC-NEW
MS
OTAPA IS PENDING
CLEAR PENDING FLAG
REGCANC
regconc[otapa_pending,otafaddr]
REGCANC
regconc
SET OTAPA PENDING FLAG
STORE OTAF ADDR
REGNOT
regnot
REGNOT[syscap]
regnot
MSC IS NOT
OTAPA-CAPABLE
REGISTRATION

FIG. 19

FIG. 20

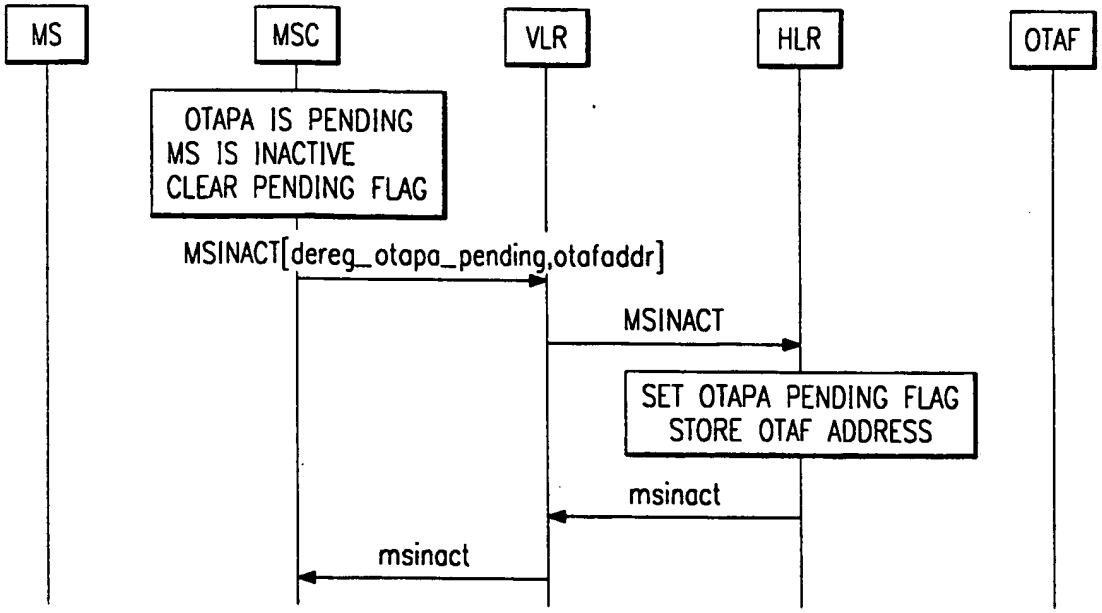

MS
MSC
VLR
HLR
OTAF
OTAPA IS PENDING
MS IS INACTIVE
CLEAR PENDING FLAG
MSINACT[dereg_otapa_pending,otafaddr]
MSINACT
SET OTAPA PENDING FLAG
STORE OTAF ADDRESS
msinact
msinact

FIG. 21

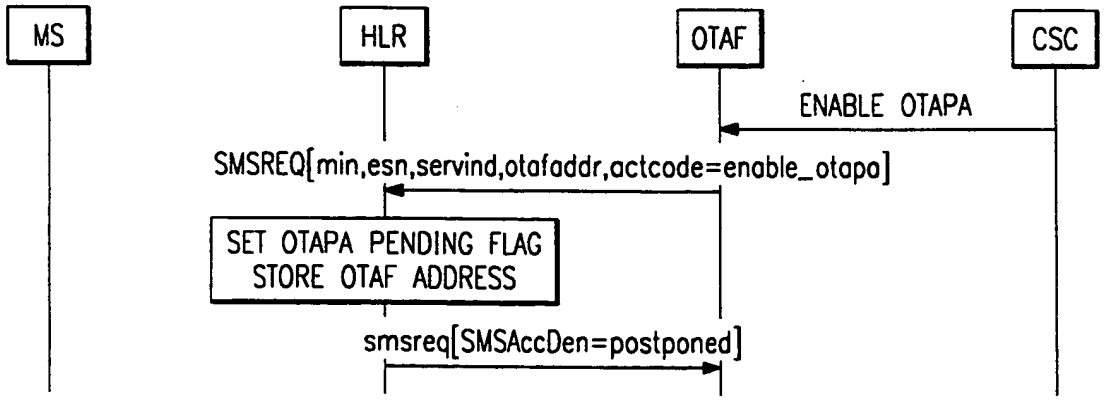

MS
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ[min,esn,servind,otafaddr,actcode=enable_otapa]
SET OTAPA PENDING FLAG
STORE OTAF ADDRESS
smsreq[SMSAccDen=postponed]

FIG. 22

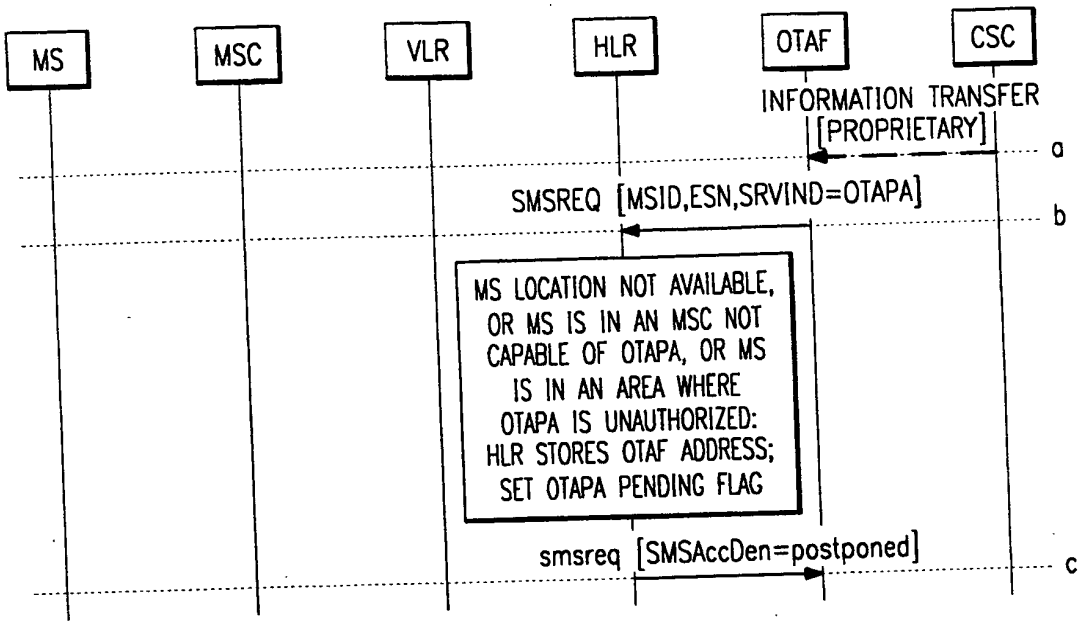


FIG. 23

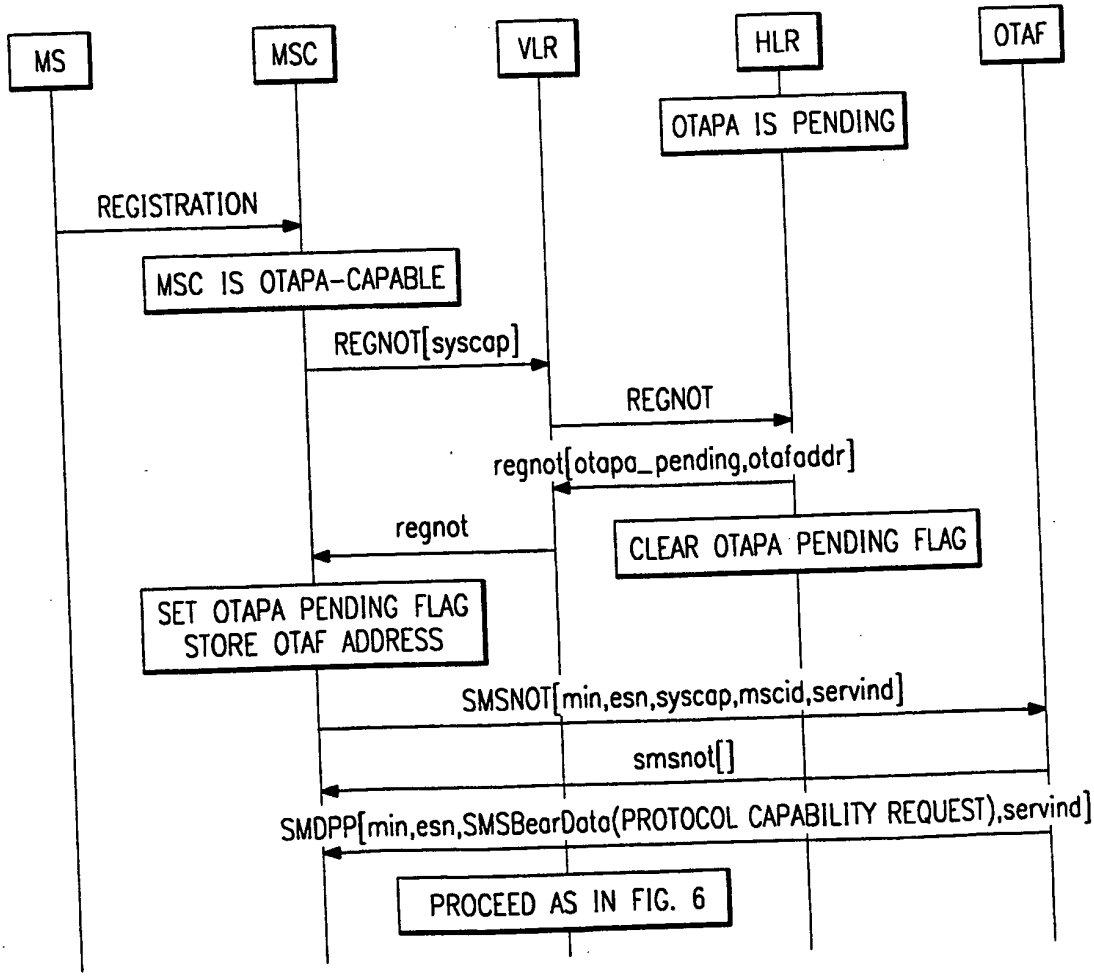


FIG. 24

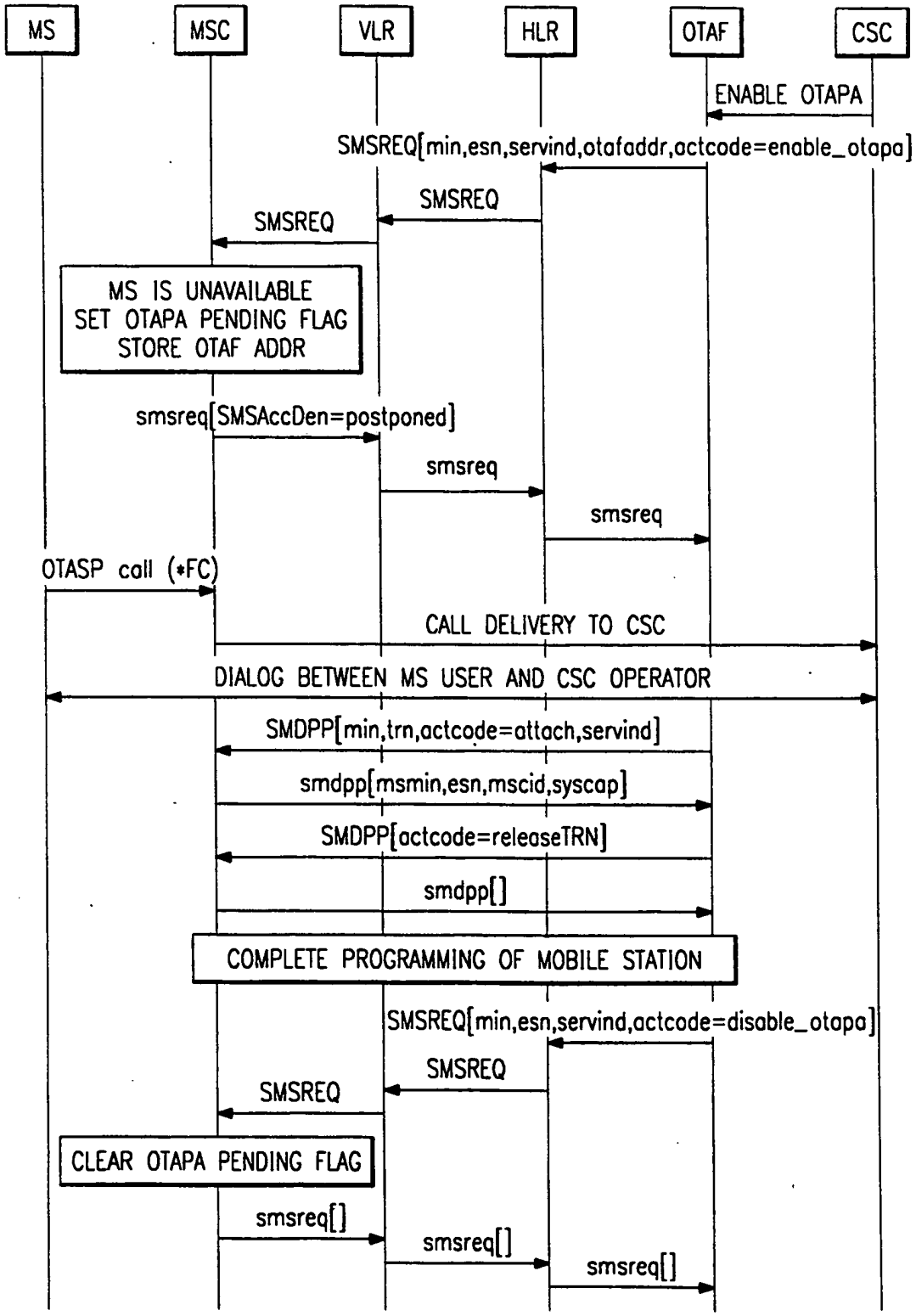

MS
MSC
VLR
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ[min,esn,servind,otafaddr,actcode=enable_otapa]
SMSREQ
SMSREQ
MS IS UNAVAILABLE
SET OTAPA PENDING FLAG
STORE OTAF ADDR
smsreq[SMSAccDen=postponed]
smsreq
smsreq
OTASP call (*FC)
CALL DELIVERY TO CSC
DIALOG BETWEEN MS USER AND CSC OPERATOR
SMDPP[min,trn,actcode=attach,servind]
smdpp[msmin,esn,mscid,syscap]
SMDPP[actcode=releaseTRN]
smdpp[]
COMPLETE PROGRAMMING OF MOBILE STATION
SMSREQ[min,esn,servind,actcode=disable_otapa]
SMSREQ
SMSREQ
CLEAR OTAPA PENDING FLAG
smsreq[]
smsreq[]
smsreq[]

FIG. 25

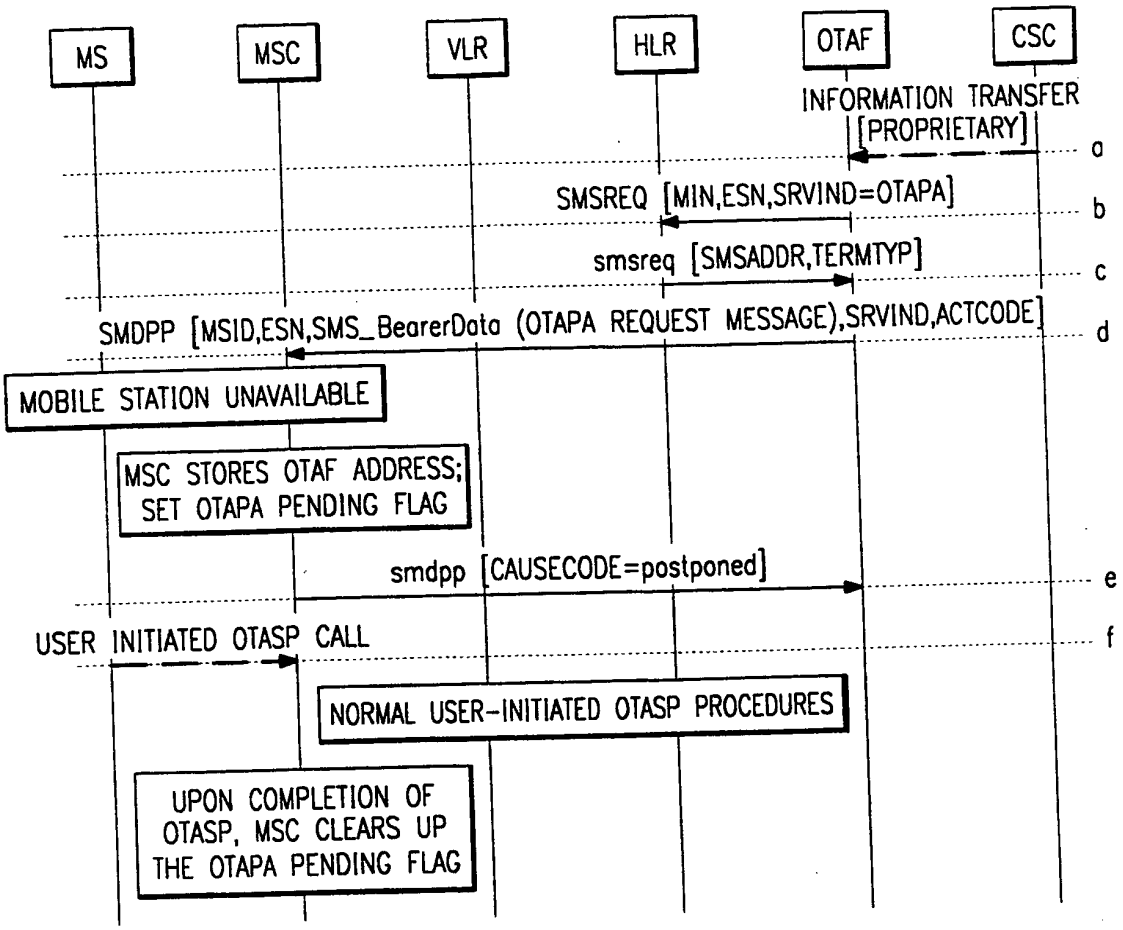

MS
MSC
VLR
HLR
OTAF
CSC
INFORMATION TRANSFER [PROPRIETARY]
a
SMSREQ [MIN,ESN,SRVIND=OTAPA]
b
smsreq [SMSADDR,TERMTYP]
c
SMDPP [MSID,ESN,SMS_BearerData (OTAPA REQUEST MESSAGE),SRVIND,ACTCODE]
d
MOBILE STATION UNAVAILABLE
MSC STORES OTAF ADDRESS; SET OTAPA PENDING FLAG
smdpp [CAUSECODE=postponed]
e
USER INITIATED OTASP CALL
f
NORMAL USER-INITIATED OTASP PROCEDURES
UPON COMPLETION OF OTASP, MSC CLEARS UP THE OTAPA PENDING FLAG

FIG. 26

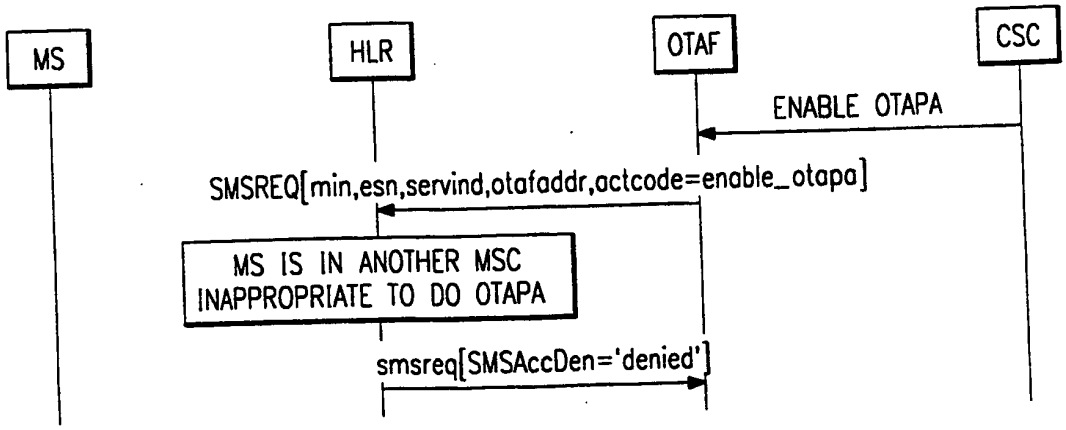

MS
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ[min,esn,servind,otafaddr,actcode=enable_otapa]
MS IS IN ANOTHER MSC INAPPROPRIATE TO DO OTAPA
smsreq[SMSAccDen='denied']

FIG. 27

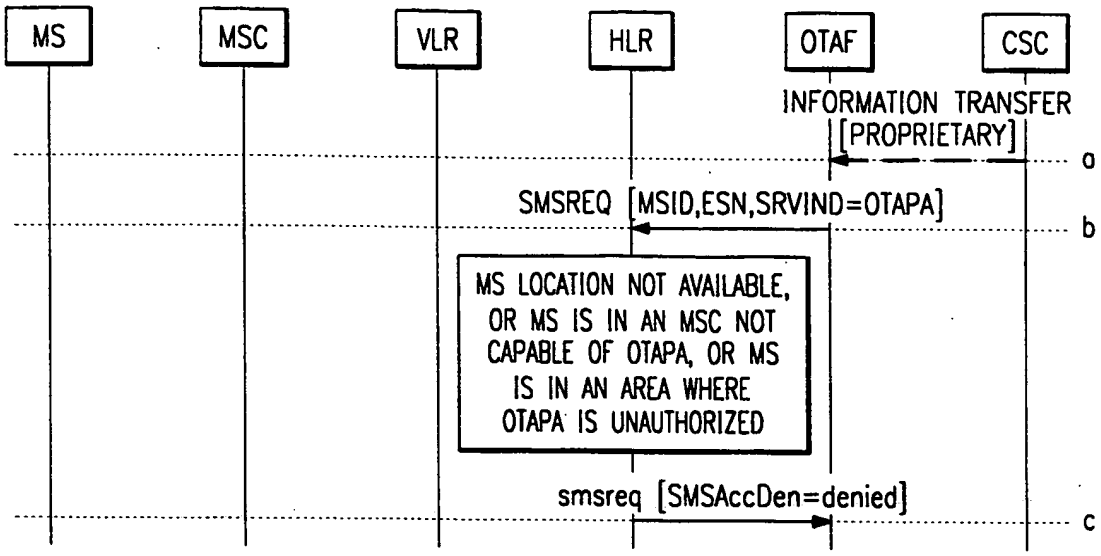
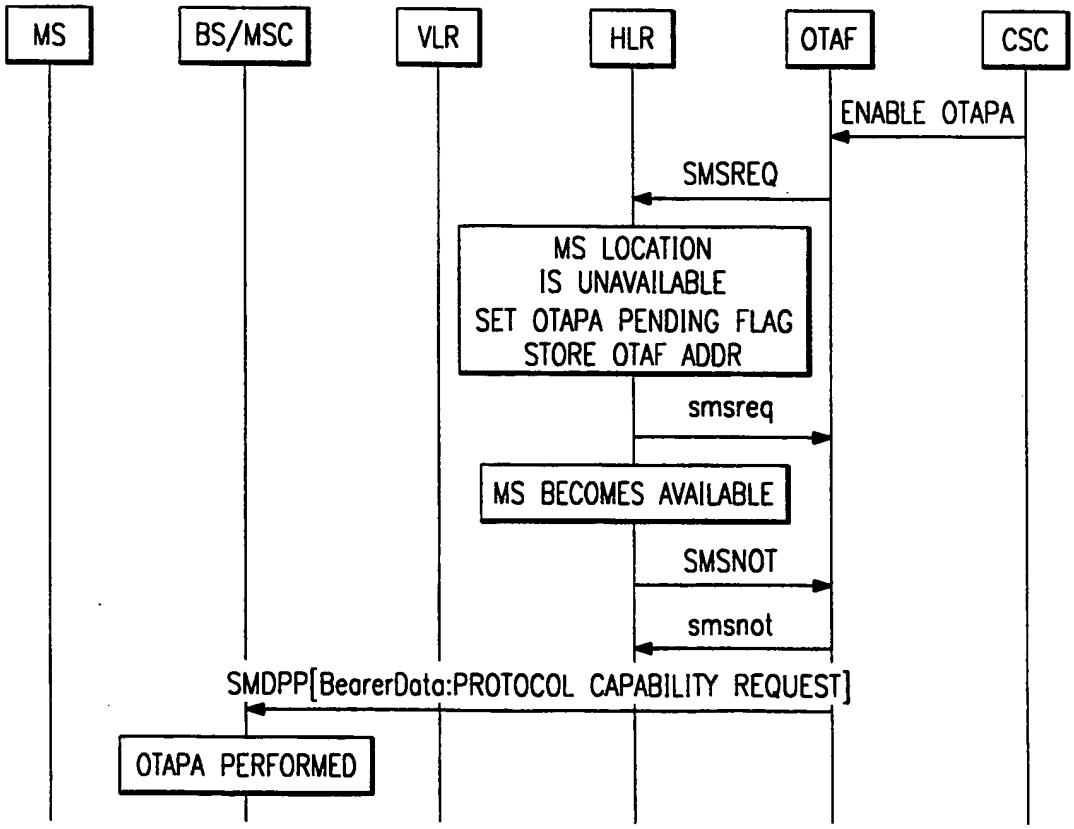

MS
MSC
VLR
HLR
OTAF
CSC
INFORMATION TRANSFER
[PROPRIETARY]
a
SMSREQ [MSID,ESN,SRVIND=OTAPA]
b
MS LOCATION NOT AVAILABLE,
OR MS IS IN AN MSC NOT
CAPABLE OF OTAPA, OR MS
IS IN AN AREA WHERE
OTAPA IS UNAUTHORIZED
smsreq [SMSAccDen=denied]
c

FIG. 28


MS
BS/MSC
VLR
HLR
OTAF
CSC
ENABLE OTAPA
SMSREQ
MS LOCATION
IS UNAVAILABLE
SET OTAPA PENDING FLAG
STORE OTAF ADDR
smsreq
MS BECOMES AVAILABLE
SMSNOT
smsnot
SMDPP[BearerData:PROTOCOL CAPABILITY REQUEST]
OTAPA PERFORMED

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/32

A3

(11) International Publication Number: **WO 98/41044**

(43) International Publication Date: 17 September 1998 (17.09.98)

(21) International Application Number: PCT/US98/05096

(22) International Filing Date: 13 March 1998 (13.03.98)

(30) Priority Data:
60/041,093 14 March 1997 (14.03.97) US

(71) Applicant: NORTHERN TELECOM INC. [US/US]; 2221 Lakeside Boulevard, Richardson, TX 75082-4399 (US).

(72) Inventors: YAU-FAN, Leung; 1604 Belgrade Drive, Plano, TX 75023 (US). DENMAN, Robert, E.; 2420 San Gabriel Drive, Plano, TX 75074 (US). WAMBSGANZ, Kevin; 1809 Papeete Drive, Plano, TX 75075 (US). CHANG, Kim; 3114 Park Gark Place, Richardson, TX 75082 (US).

(74) Agent: CARR, Gregory, W.; Winstead Sechrest & Minick P.C., 5400 Renaissance Tower, 1201 Elm Street, Dallas, TX 75270-2199 (US).

(81) Designated States: JP, KR.

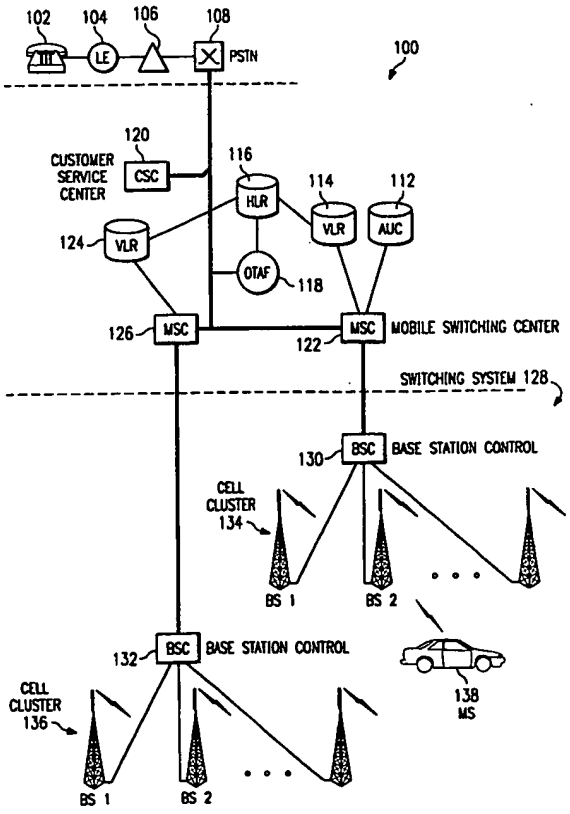
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
14 January 1999 (14.01.99)

(54) Title: METHOD AND APPARATUS FOR NETWORK INITIATED PARAMETER UPDATING

(57) Abstract

Disclosed is an apparatus for initiating an over the air parameter administration (OTAPA) of a mobile station without the need for interacting with a mobile station user. A unique service option number included with the initial page indicates to the mobile station that an update is being requested. The mobile station performs a network validation check (SPASM) before permitting the update to take place. Flags are used in the network to alert the system that an attempted update was not completed because a mobile station was not update accessible for any of several reasons. The flags cause the system to update when the mobile station next becomes update accessible.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

INTERNATIONAL SEARCH REPORT

Ir. ational Application No
PCT/US 98/05096

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/32

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 722 084 A (CHAKRIN ET AL.) 24 February 1998 see column 2, line 1 - column 4, line 13; figures ---	1,4,6,8, 10,12,23
X	WO 96 27270 A (ERICSSON) 6 September 1996 see page 8, line 19 - page 20, line 10; figures ---	1,4,6,8, 10,12,23
X	DE 196 33 919 C (SIEMENS) 5 June 1997 see column 1, line 62 - column 3, line 55; figure ---	21,22
A	EP 0 767 426 A (SIEMENS) 9 April 1997 see page 2, line 1 - page 4, line 20; figures --- -/--	1-20

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
23 November 1998	30/11/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Geoghegan, C

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/05096

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 675 661 A (ALCATEL) 4 October 1995 see page 2, column 2, line 47 - page 4, column 5, line 18; figures	1-10
A	EP 0 478 231 A (AT&T) 1 April 1992 see page 4, line 14 - page 6, line 43; figures	1-20
A	EP 0 459 344 A (ALCATEL) 4 December 1991 see page 3, column 3, line 31 - page 5, column 8, line 34; figures	1-20
A	DE 43 21 381 A (ALCATEL) 5 January 1995 see column 2, line 21 - column 3, line 66; figures	21,22

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/05096

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5722084 A	24-02-1998	US 5297192 A	22-03-1994
		US 5297191 A	22-03-1994
		CN 1101469 A	12-04-1995
		EP 0630167 A	21-12-1994
		JP 7107187 A	21-04-1994
		CA 2045801 A,C	29-03-1992
		DE 69124445 D	13-03-1997
		DE 69124445 T	26-06-1997
		EP 0478231 A	01-04-1992
		ES 2096631 T	16-03-1997
		JP 2593599 B	26-03-1997
		JP 6343108 A	13-12-1994
		CA 2045800 A,C	29-03-1992
		JP 2801445 B	21-09-1998
		JP 6284078 A	07-10-1994
WO 9627270 A	06-09-1900	US 5603084 A	11-02-1997
		AU 5300896 A	18-09-1996
		CA 2213464 A	06-09-1996
		CN 1182522 A	20-05-1998
DE 19633919 C	05-06-1997	NONE	
EP 767426 A	09-04-1900	NONE	
EP 675661 A	04-10-1995	FR 2718263 A	06-10-1995
		AU 698341 B	29-10-1998
		AU 1612395 A	12-10-1995
		CA 2145602 A	01-10-1995
		FI 951493 A	01-10-1995
		JP 7271692 A	20-10-1995
		NZ 270702 A	29-01-1997
EP 478231 A	01-04-1992	CA 2045800 A,C	29-03-1992
		DE 69124445 D	13-03-1997
		DE 69124445 T	26-06-1997
		ES 2096631 T	16-03-1997
		JP 2801445 B	21-09-1998
		JP 6284078 A	07-10-1994
		US 5297191 A	22-03-1994
		US 5722084 A	24-02-1998
		CA 2045801 A,C	29-03-1992
		JP 2593599 B	26-03-1997
		JP 6343108 A	13-12-1994
		US 5297192 A	22-03-1994
EP 459344 A	04-12-1991	FR 2662891 A	06-12-1991
		AU 643526 B	18-11-1993
		AU 7739591 A	05-12-1991
DE 4321381 A	05-01-1995	NONE	